

## SOFTWARE OUTPUT

Launching appinitdlls v.20130425

appinitdlls v.20130425

(Software) Gets contents of AppInit\_DLLs value

AppInit\_DLLs

Microsoft\Windows NT\CurrentVersion\Windows

LastWrite Time Tue Jul 14 04:53:25 2009 (UTC)

AppInit\_DLLs : {blank}

LoadAppInit\_DLLs : 0

\*LoadAppInit\_DLLs value globally enables/disables AppInit\_DLLS.

0 = disabled (default)

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows

LastWrite Time Tue Jul 14 04:53:25 2009 (UTC)

AppInit\_DLLs : {blank}

LoadAppInit\_DLLs : 0

\*LoadAppInit\_DLLs value globally enables/disables AppInit\_DLLS.

0 = disabled (default)

Analysis Tip: The AppInit\_DLLs value should be blank; any DLL listed is launched with each user-mode process.

-----  
 apppaths v.20120524

(Software) Gets content of App Paths subkeys

App Paths

Microsoft\Windows\CurrentVersion\App Paths

Sun Mar 27 02:09:38 2016 (UTC)

vimtag.exe - C:\Program Files (x86)\Vimtag\vimtag.exe

Sat Feb 20 02:05:23 2016 (UTC)

VMidi.exe - C:\Program Files (x86)\vanBasco's Karaoke Player\VMidi.exe

Tue Feb 2 00:21:28 2016 (UTC)

PDFPlus.exe - C:\Program Files (x86)\Nuance\PDF Viewer Plus\Bin\PDFPlus.exe

Tue Feb 2 00:19:30 2016 (UTC)

PaprPort.exe - C:\Program Files (x86)\Nuance\PaperPort\PaprPort.exe

Thu Jan 14 16:38:24 2016 (UTC)

msoxmled.exe - C:\Program Files (x86)\Common Files\Microsoft

Shared\OFFICE12\MSOXMLED.EXE

Thu Jan 7 22:15:24 2016 (UTC)

iTunes.exe - C:\Program Files\iTunes\iTunes.exe

Thu Jan 7 22:07:26 2016 (UTC)

QuickTimePlayer.exe - C:\Program Files (x86)\QuickTime\QuickTimePlayer.exe

Fri Jan 1 20:52:20 2016 (UTC)

firefox.exe - C:\Program Files (x86)\Mozilla Firefox\firefox.exe

Sat Sep 12 03:23:06 2015 (UTC)

mbam.exe - C:\Program Files (x86)\Malwarebytes Anti-Malware\mbam.exe

Fri Sep 11 14:57:00 2015 (UTC)

## SOFTWARE OUTPUT

chrome.exe - C:\Program Files (x86)\Google\Chrome\Application\chrome.exe  
 Thu Sep 10 21:40:41 2015 (UTC)  
 vstoee.dll -  
 Thu Sep 10 21:32:13 2015 (UTC)  
 ois.exe - C:\PROGRA~2\MICROS~2\Office14\OIS.EXE  
 Thu Sep 10 21:32:12 2015 (UTC)  
 MsoHtmEd.exe -  
 OUTLOOK.EXE - C:\PROGRA~2\MICROS~2\Office14\OUTLOOK.EXE  
 Thu Sep 10 19:07:29 2015 (UTC)  
 WinRAR.exe - C:\Program Files\WinRAR\WinRAR.exe  
 Thu Sep 10 16:33:31 2015 (UTC)  
 Winword.exe - C:\PROGRA~2\MICROS~2\Office12\WINWORD.EXE  
 Thu Sep 10 16:33:30 2015 (UTC)  
 excel.exe - C:\PROGRA~2\MICROS~2\Office12\EXCEL.EXE  
 OneNote.exe - C:\PROGRA~2\MICROS~2\Office12\ONENOTE.EXE  
 powerpnt.exe - C:\PROGRA~2\MICROS~2\Office12\POWERPNT.EXE  
 Thu Sep 10 16:25:03 2015 (UTC)  
 PhotoshopElements.exe - C:\Program Files (x86)\Adobe\Photoshop Elements  
 2\PhotoshopElements.exe  
 Mon Dec 1 14:13:22 2014 (UTC)  
 IEDIAG.EXE - C:\Program Files\Internet Explorer\IEDIAGCMD.EXE  
 IEDIAGCMD.EXE - C:\Program Files\Internet Explorer\IEDIAGCMD.EXE  
 IEXPLORE.EXE - C:\Program Files\Internet Explorer\IEXPLORE.EXE  
 Mon Dec 1 12:59:32 2014 (UTC)  
 fsquirt.exe -  
 Mon Dec 1 12:56:41 2014 (UTC)  
 cmmgr32.exe -  
 Tue Apr 12 08:28:59 2011 (UTC)  
 dvdmaker.exe - %ProgramFiles%\DVD Maker\dvdmaker.exe  
 Journal.exe - %ProgramFiles%\Windows Journal\Journal.exe  
 mip.exe - %CommonProgramFiles%\Microsoft Shared\Ink\mip.exe  
 SnippingTool.exe - %SystemRoot%\system32\SnippingTool.exe  
 TabTip.exe - %CommonProgramFiles%\microsoft shared\ink\TabTip.exe  
 Tue Jul 14 04:53:25 2009 (UTC)  
 install.exe -  
 migwiz.exe -  
 mplayer2.exe - %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe  
 pbrush.exe - %SystemRoot%\System32\mspaint.exe  
 PowerShell.exe - %SystemRoot%\system32\WindowsPowerShell\v1.0\PowerShell.exe  
 setup.exe -  
 sidebar.exe - "%ProgramFiles%\Windows Sidebar\sidebar.exe"  
 table30.exe -  
 wab.exe - %ProgramFiles%\Windows Mail\wab.exe  
 wabmig.exe - %ProgramFiles%\Windows Mail\wabmig.exe  
 wmplayer.exe - %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe  
 WORDPAD.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"  
 WRITE.EXE - "%ProgramFiles%\Windows NT\Accessories\WORDPAD.EXE"  
 Wow6432Node\Microsoft\Windows\CurrentVersion\App Paths not found.

## SOFTWARE OUTPUT

-----  
assoc v.20080815

(Software) Get list of file ext associations

assoc

Classes

-----  
banner v.20081119

(Software) Get HKLM\SOFTWARE.. Logon Banner Values

Logon Banner Information

Microsoft\Windows\CurrentVersion\policies\system

LastWrite Time Sun Dec 13 17:44:46 2015 (UTC)

Legalnoticecaption value =

Legalnoticetext value =

Microsoft\Windows NT\CurrentVersion\Winlogon

LastWrite Time Wed Apr 20 02:36:52 2016 (UTC)

Legalnoticecaption value =

Legalnoticetext value =

-----  
bho v.20130408

(Software) Gets Browser Helper Objects from Software hive

Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects

LastWrite Time Sun Feb 21 01:14:20 2016 (UTC)

{B4F3A835-0E21-4959-BA22-42B3008E02FF}

Class =&gt; Office Document Cache Handler

Module =&gt; C:\PROGRA~1\MICROS~2\Office14\URLREDIR.DLL

LastWrite =&gt; Thu Sep 10 21:28:34 2015

Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects

LastWrite Time Sun Feb 21 01:14:20 2016 (UTC)

Classes\CLSID\{551A852F-39A6-44A7-9C13-AFBEC9185A9D} not found.

{B4F3A835-0E21-4959-BA22-42B3008E02FF}

Class =&gt; Office Document Cache Handler

Module =&gt; C:\PROGRA~1\MICROS~2\Office14\URLREDIR.DLL

LastWrite =&gt; Thu Sep 10 21:28:34 2015

## SOFTWARE OUTPUT

-----  
bitbucket v.20080418

(Software) Get HKLM\..\BitBucket keys\values

Microsoft\Windows\CurrentVersion\Explorer\BitBucket not found.  
-----

clsid v.20130603

(Software) Get list of CLSID/registered classes

Classes\CLSID

Wed Apr 20 02:37:17 2016 Z

{0F5FA46A-D17B-4978-8A4C-65474C8DF59F}	SaSubMgr Class
{5A90F5EE-16B8-4C2A-81B3-FD5329BA477C}	McAfee SACore Component
{CD009C4C-EAAC-4A03-9C44-4342D4CFABA9}	McAfee Host SA Plugin

Tue Apr 19 01:22:02 2016 Z

{9EBE7B1C-29B4-457A-A4FF-2883604805E0}	McAfee VSCore Version Class
--	-----------------------------

Tue Apr 19 01:21:58 2016 Z

{A95B959F-64A9-43E4-A874-C8A77905854A}	CMcSvcHostVer Class
--	---------------------

Tue Apr 19 01:21:53 2016 Z

{132DB361-34A1-43A3-9ECC-5BE245730365}	CoMcAlertMgr Class
{45F5697C-8C8C-4FDF-994E-C452372992E0}	CoAlertMgrAutomation Class

Tue Apr 19 01:21:50 2016 Z

{20966775-18A4-4299-B8E3-772C336B52A7}	McSurrogateHelper Class
{3BAC5BDD-FCA1-4E2F-9062-6693E80016D8}	McPlatformServiceFramework Class
{4B3DBDAB-C46F-40D3-A415-3DB9585F4D00}	McUtilProvider Class
{85C12AD0-200B-48A0-9BEF-880ED5BE9D1D}	McPlatformService Class
{C307ED64-2933-4E7E-869B-7EFC8F6C7B18}	McAMTask Class

Tue Apr 19 01:21:35 2016 Z

{6641D86E-79C2-42ED-9C08-BBDA2B780E1D}	PEFWebObjects Class
{B97FDD09-7004-437E-9D5F-D336CB0F31A0}	CoUpdateMgrNotifyImpl Class

Tue Apr 19 01:21:34 2016 Z

{E8C19781-29C1-4B08-9004-4F1BF947CCE9}	PCSystem Class
{ED71209D-F723-4ACB-BE33-1E5A79F9FEF3}	PCFile Class

Tue Apr 19 01:21:33 2016 Z

{100A0E8F-D705-44AA-ABA7-842B96FA4ED9}	PEFSubDB Class
{B345DB9D-2FBE-4267-ADA2-5EFBFBF9C42F}	PCRegistry Class
{DE4B86D4-00A1-463A-A26E-B7E555482952}	PefIntegration Class

Tue Apr 19 01:20:17 2016 Z

{255A5958-D283-4DD9-AA2E-8E33805CFC35}	McCSPClientAutomation Class
{8F2BC96B-68C5-40E8-9CE1-368E3ACAC09B}	McCSPClientShim Class
{A2476F99-46DE-4B6A-BC65-2BA13F8EC016}	McAnalyticsShim Class
{A759F428-E51D-4CDF-8E4C-A52B7F9927D0}	McCDCObject Class
{B62A9F7D-4F97-4740-9EEE-3554F2AD2E4B}	McCSPClient Class
{E7BAC6B6-3FE3-4761-9471-F8F2C38C6C47}	McCDCObjectShim Class

Tue Apr 19 01:20:16 2016 Z

{ED811A7F-3DA0-48C9-BF42-9F7838F7471B}	McAnalytics Class
--	-------------------

Tue Apr 19 01:20:13 2016 Z



## SOFTWARE OUTPUT

{3C6B7AB4-14F6-49FA-93B2-536A7374C83A} CUninstallCustomization Class  
 {524FFCA8-CE5C-4D65-A78F-716D1A403B1E} CoMcServerContent Class  
 Tue Apr 19 01:20:10 2016 Z  
 {CCA9EFD3-29ED-430A-BA6D-E6BBFF0A60C2} McCtxFrmWrk Class  
 Tue Apr 19 01:20:09 2016 Z  
 {39BE9FE5-916F-4F01-86D8-46D1B843C8DD} CCoMcApplicationInfo Class  
 {3EF5086B-5478-4598-A054-786C45D75692} McInternetProtocolRoot Class  
 {F6F390DB-9953-497B-B2F8-9F9B7C8A1B1C} McUninstaller Class  
 Tue Apr 19 01:20:08 2016 Z  
 {9BB86057-19A1-49BB-A522-D4CE0AF55767} CoMcIPTMgr Class  
 {A557A096-4DA4-4E32-B863-BAFD39EEB367} McPersonalization Class  
 Tue Apr 19 01:20:07 2016 Z  
 {2670E39B-AD89-451F-8220-DD8FC72E74D6} McHistoryAndLogs Class  
 {4FE2B7C8-AC9D-473C-A227-528F96CF0A88} CoMcTOC Class  
 {562E13B7-17D5-4393-A51E-BF1EFCB2AB13} CoMcMLSMTKInfo Class  
 {678BABB8-FE1A-40A6-BB51-DFBF5F902E02} CoMcReport Class  
 {A3D27DAD-37A4-496A-9553-2BD3E856899C} CoMcMLSProv Class  
 {F5DDF629-FAC9-4AA5-9BFF-EDA5FF8026AB} CoMcTaskScheduler Class  
 Tue Apr 19 01:20:06 2016 Z  
 {071345B6-580F-47e5-A454-A76E9817CD8D} CoMcAboutInfoCShim Class  
 {3ED11E13-AB3A-49A1-B29E-B33853F6CB4A} McUpdateSettings Class  
 {57249F09-6C95-43D5-977C-301EBAF7F3F5} CoMcSecurityCenter Class  
 {5744BAD0-CB1D-43DB-90BD-1D2778CB0AD8} CoMcMSCMiscellaneous Class  
 {72FA3944-C398-4300-BFAF-00F83A7F1B3E} McMscHelper Class  
 {7B3BE4B3-1ACA-40A1-B056-E01874B94975} CoMcCategories Class  
 {9BE580F3-3B6B-4101-923B-7D74D0D82B04} CoMcProvHome Class  
 {AD6E7ABF-E06F-4ff6-B734-D04F22DAE042} CoMcMscCShim Class  
 {B7D66A11-7233-4e29-A3B7-9D359344ED5B} CoMcInfoviz Class  
 Tue Apr 19 01:20:05 2016 Z  
 {26608B46-476A-4bf1-9CC6-AFEA28EBBC17} McUserManager Class  
 {4D8E7AFE-514C-40eb-BBCB-ED0806F2E47E} McEventDatabaseManager Class  
 {5A40054F-2EBB-41bd-8A94-38C91AAFBC43} McLogDatabaseManager Class  
 {8472B0B6-1510-4c08-B72F-1005782AF3D2} McReportRecentEvent Class  
 {BF1A6196-0201-41FF-9024-EBDCA65A2D85} McGensettings Class  
 {DDC6C82A-BCD6-480f-BAE7-9F406F687A53} McReportLog Class  
 {EC5F8EE1-A52B-4841-85C2-362990D50919} CoMcCloudEventData Class  
 Tue Apr 19 01:20:01 2016 Z  
 {209500FC-6B45-4693-8871-6296C4843751} ProtectionUIManager Class  
 {211EBA3A-EA5A-496b-A021-5C6BEB365E4C} McAfee VirusScan ActiveShield  
 Tue Apr 19 01:20:00 2016 Z  
 {6DFC2D17-579D-4c1c-93B7-B05B7DCCD766} CoMcUpdateUI Class  
 {8F7EE58B-CEA5-4869-962F-AD58E4BD7465} CoMcUpdateClientUI Class  
 {ADA518B9-B7A3-4C36-B4ED-49EB3FA189FC} CoUpdateConnector Class  
 {E001E795-5A24-4E12-8B9C-6B80F190767D} CoMcUpdateClient Class  
 {F01E4065-20D6-4c86-9076-468AFB1B4156} SessionMgr Class  
 Tue Apr 19 01:19:59 2016 Z  
 {E0EC0F2B-773D-4dd7-BE6C-7D85D6AA6269} McAfee Agent  
 Tue Apr 19 01:19:48 2016 Z

## SOFTWARE OUTPUT

```

{05C25B6F-5FC4-4E03-A330-F0F205FB2E9D} CoMcTelemetryAPIShm Class
{495DC25F-9EDE-47B4-968D-445A91B5C73E} McSMPProvider Class
{78EFC69B-FD0E-4F47-90D6-2FAD478C468D} McDspRegistry Class
{A8C5E344-038D-46D8-8B41-AED5C5BC9905} McDspDatabaseMgr Class
{D8736336-1BE6-4B07-82ED-76995CE281DE} McDspFileSystem Class
{DF659FF1-A244-4D36-9F84-75BB2D03EB2E} McMschHelper Class
{E66D03F6-C1CF-4D8C-997C-FAE8763375F6} ManageOem Class
{EEDAC291-85BC-488F-92DF-BA392D4AC6DE} McDspSystemInfo Class
Tue Apr 19 01:19:45 2016 Z
{1DD7B920-0AAE-457B-8A6B-077A92933F82} McSvcSubsystem Class
Tue Apr 19 01:19:42 2016 Z
{07AA2658-7A1A-47e5-B01A-701DC9EECD6F} McHackerWatchFirewallSettings Class
{0CE809D3-1D8B-4321-9F89-3F49CEA8B15C} McHackerWatchServerQuery Class
{231727DB-4A5A-4c85-B844-64E3A30BE7A3} McHackerWatchAppDetails Class
{36C29AB6-FF73-4f74-A2D1-C5C09B54E5C9} McHackerWatch Class
{6021CE48-B556-4f11-BC68-A647F056F8CC} McHackerWatchVersion Class
{85DADE1D-E53C-4E3A-8514-19FFB6B00423} McHackerWatchAppEntry Class
{A0EBB878-FDC0-4514-AEE9-F68E4337E7D2} McHackerWatchSettings Class
{FB49CFE3-C775-48f1-B0C6-BEBABF84EFF9} McHackerWatchSharedPerms Class
Tue Apr 19 01:19:34 2016 Z
{090C890A-8E62-4324-954D-BCD2DFBE4E12} Network Class
{296CFB80-D8B3-44A4-B6B8-1931267F8F11} ShimCallback Class
{81375E2A-DBC6-4F93-A221-5DEE92D3A34C} ShimList Class
{89105939-0E55-4F63-82F2-7EF170402AD1} McAfee HomeNetwork Shim Component
{AF0CE3EB-8E31-4D61-98D4-A047F4826DE8} ShimNetworkNode Class
{BBEDBE75-6E9C-40CB-8D3C-681E9F03807E} McAfee HomeNetwork Service Module
{C28D8A9A-B234-4B23-8E31-1F4D1B9450CE} ShimDynamicAttribute Class
{CBC58E3D-6DF2-4187-8188-CF9C261F1B89} ShimProtectionProblem Class
{CEEEE239-EBC4-4780-A9EA-832D4634BCEC} CoAlertLauncher Class
Tue Apr 19 01:19:33 2016 Z
{169C3F7A-F974-4B6B-BF09-DD7D08EAC3CE} HomeNetVer Class
Wed Apr 6 19:30:37 2016 Z
{15AF52F6-E83C-4228-95FE-4407687CEFBF} CoMcUpdAgentUIHandler Class
{3C1CD4CD-9359-4A9D-A0FA-9E809E873CA6} CoMcUpdateAgentCore Class
{DA32C9C5-1147-402A-A127-E0E169E9E9B4} CoMcUpdateAgent Class
Wed Apr 6 19:30:36 2016 Z
{D905F5A4-15B0-4B47-99D8-CE0230557148} CoUpdateMgrCore Class
Mon Mar 21 20:51:23 2016 Z
{76DEF3AC-2910-4234-9EE2-C81B2D45833A} McAfee VirusScan Alerter
Mon Mar 21 20:51:22 2016 Z
{84D248DA-52CD-442c-B6AE-28F143DB1E33} CoMcVSQuarantineAx Class
{C98F04D7-CD30-4bb0-B7D7-8DD7448520F2} McAfee MCODS
Mon Mar 21 20:51:21 2016 Z
{01576F39-90DE-4D6E-A068-5B20C22BAEEE} CtxMenu Class
Mon Mar 21 20:51:19 2016 Z
{395633B1-EED9-4DFC-B67F-9788B51C9F06} McAfee VirusScan Announcer Administrative
Class
{44603E4D-56AE-4c42-ABE4-EC155FE8F1CD} McAfee VirusMap Reporting

```

## SOFTWARE OUTPUT

```

{782C48A5-DD18-43E5-B32E-88E66CBB85D0} McAfee VirusScan Announcer Alerter Class
{A737699F-3765-4B1D-ADAF-77424E23A9FA} McAfee VirusScan Announcer Subsystem Class
{C90134D2-4AE9-407A-919A-4A2EF09C6C51} MfeVsAnnServiceConfig Class
{DC7EF8E1-824F-4110-AB43-1604DA9B4F40} McAfee VirusScan Announcer State Class
Mon Mar 21 20:50:17 2016 Z
{9BE8D7B2-329C-442A-A4AC-ABA9D7572602} McSubMgr Class
Mon Mar 21 20:50:16 2016 Z
{61B085E5-356C-4fed-BEFF-AC6BE240B548} CoMcApplicationRegistration Class
{89CA5F54-B963-4092-873A-AFE498746367} CoMcProviderRegistration Class
{F2E467DC-4C6D-497c-A629-796B8CBF7275} CoMcLogTemplateRegistration Class
Sat Mar 12 23:51:19 2016 Z
{861CEB0E-B6F3-4DA8-A7E7-DBC43D335628} PSFactoryBuffer
{8DFD2991-CE6C-403C-B287-94E7F0D5BA07} PSFactoryBuffer
Sat Feb 20 01:47:12 2016 Z
{60260024-AA48-4A2F-84DA-2C2DCB24AAD0} CHttpMonitor Object
{82025773-B1B0-497b-B942-0171A2E42C3C} CHttpHeadersImpl Object
Fri Feb 19 09:25:07 2016 Z
{B970338F-FDF9-45A2-B3F5-586C61BF5C1D} McSvcSubsystem Class
Fri Feb 19 09:25:06 2016 Z
{19A34F98-20C0-4449-A3B4-29071BCEAD91} MskOLAddIn Class
{C438913D-25B3-48cf-9310-9422CBCB19AB} MskPlugin
Fri Feb 19 09:25:03 2016 Z
{3087BEE5-7B7F-4C66-AB0B-5DCC65CD48A2} CoMcAntispam Class
{516A0FE6-CA82-49F9-97EF-B5091F4B2E5A} MskProtection Class
Fri Feb 19 09:25:02 2016 Z
{45559631-986C-4546-87E1-8AE1F9614296} MSKSrgHelper Class
Fri Feb 19 09:25:00 2016 Z
{447CAE10-7647-45f9-9AD8-68243ED5A2DA} MpfMcApplicationInfoProviderImpl Class
{820B1F90-F6DF-4f3a-9658-2A2E12F7B57C} MpfMcLogActionProviderImpl Class
{BD7EC3D0-8A8F-4ab8-9070-07997206D505} MpfMcRecentEventActionProviderImpl Class
Fri Feb 19 09:24:59 2016 Z
{5B2BB965-9043-498C-B60E-C0379DC0BBD4} TrafficMonitor Class
{7585011C-0545-4F40-86B2-07639245F8ED} MpfNdHelper Class
{83EEF1DB-16A2-426F-843D-85A5348337C1} MpfSvcImpl Class
{90DBDD22-4A4A-4b23-8BBC-969C9869E1D6} MpfAPIImpl Class
{C13F71BC-CC67-40A4-BEF2-1CBF44BD2A6D} McAfee Personal Firewall MISP Alert
{C74C7A1D-476C-482A-B9D9-D76B50AFFFD4} FirewallSettings Class
Fri Feb 19 09:24:58 2016 Z
{01A3B960-21A7-4231-909E-7597D17EF4A5} McAfee Personal Firewall Application Class
{AAC05D4F-D3FC-4d85-B706-55ECE9CE6DCA} McAfee Personal Firewall Configuration
Class
{BA041363-3548-4CBA-BDB8-9338683BB8BC} McAfee Personal Firewall Version Class
{F8FDC79F-E062-48b0-946D-45DE13685593} McAfee Personal Firewall OEM Configuration
Class
Fri Feb 19 09:24:51 2016 Z
{4E112792-FF8F-4f97-818B-2D7B9492F897} MPFSubSystem Class
{DB4FBF4C-8F23-4FD5-97CB-84020AE74965} McMPFSvc Class
Fri Feb 19 09:20:23 2016 Z

```

## SOFTWARE OUTPUT

{2CF7C0ED-0BC8-4CA5-AB2E-798E15D6EDDB} IMcUIConfigMgr Class  
 {5268CCA1-1270-4B04-B155-BD0753440278} CompReg Class  
 Fri Feb 19 09:19:51 2016 Z  
 {AC29BAF7-7EFF-4A82-8B29-76B1A3E27A6D} PSFactoryBuffer  
 {E782BE15-9936-4A7F-8DF9-9AB95D229DF1} McClientAnalytics Class  
 Sun Feb 14 15:57:32 2016 Z  
 {5860E1C5-F95C-4a7a-8EC8-8AEF24F379A1} CplPage Class  
 Wed Feb 10 01:12:55 2016 Z  
 {2559a1f8-21d7-11d4-bdaf-00c04f60b9f0} Upgrade to Windows 10  
 {2559a1f9-21d7-11d4-bdaf-00c04f60b9f0} Upgrade to Windows 10  
 Tue Feb 9 22:20:49 2016 Z  
 {FAEA5B46-761B-400E-B53E-E805A97A543E} Microsoft Office Visio Persistent Handler  
 Thu Feb 4 14:14:42 2016 Z  
 {9D6AA569-9F30-41AD-885A-346685C74928}  
 {D580254F-5E17-4AE0-9C41-60A0526A8ED6}  
 Thu Feb 4 14:14:41 2016 Z  
 {F8BC3B89-DD15-4DA2-B936-CEA2B2A35053} PSFactoryBuffer  
 Tue Feb 2 00:28:08 2016 Z  
 {80083BF3-B821-4cc2-AC62-81FAE8D3ADCE} Brother Wia Scanner minidriver  
 Tue Feb 2 00:19:30 2016 Z  
 {5CF7CBA7-001D-4FFE-88A5-F8BBA5A6665D} PDF Professional Filter Persistent Handler  
 Tue Feb 2 00:19:23 2016 Z  
 {D7917B52-909B-4297-8649-C673F1040616}  
 Thu Jan 14 16:38:03 2016 Z  
 {DFEAF541-F3E1-4c24-ACAC-99C30715084A} Microsoft Silverlight  
 Thu Jan 7 22:40:41 2016 Z  
 {08A6AF6A-8FF2-4a3b-BECF-C2FAC8630BBF} iTunesAdminParentalControls Class  
 {20ADDA11-8287-44D0-8C63-27CDA87ACC46} iTunesAdmin Class  
 {62A560B8-09DB-4cc6-AE1B-9D8F7ADDB8F3} iTunesAdminRepairIPodSW Class  
 {6C2589C3-96F8-4863-A511-9C33EB2C7E2A} iTunesAdminAudible Class  
 {71A1A612-F7B4-4092-8E0F-C79C8FB0391D} iTunesAdminMobileDeviceService Class  
 {B8DF592B-DE05-49f5-BB21-084F548F12A9} iTunesAdminEnableAutoRun Class  
 {DC0C2640-1415-4644-875C-6F4D769839BA} iTunes Class  
 {E9D58BF1-0070-4fcd-B722-A0EE5A3ABCD6} iTunesAdminInstallTalkBackVoiceKit Class  
 {F7A782D3-2DDD-4327-BB70-0D1D0F1E38B0} iPodUpdaterInterface Class  
 Thu Jan 7 22:15:26 2016 Z  
 {B9E1D2CB-CCFF-4AA6-9579-D7A4754030EF} iTunes  
 Thu Jan 7 22:15:25 2016 Z  
 {11E4D223-C650-43F9-AB90-AB3AE4FB38F0} PSFactoryBuffer  
 Thu Jan 7 22:15:18 2016 Z  
 {063D34A4-BF84-4B8D-B699-E8CA06504DDE} iTunesService Class  
 {368F81BC-9439-41A8-B532-39C8D7E7D147} iTunesDevices Class  
 {7A7FB085-6068-4898-8CCA-480A9187277C} iPodManager Class  
 {7CCACE3-3DEE-4659-93AA-19E6C38D8EEC} ServiceDiagnostics Class  
 {B33927D0-89E6-45D8-87C7-27F3DE3EFDE6} iTunesDevicePrefs Class  
 Thu Jan 7 22:15:17 2016 Z  
 {80EE9910-D470-4AED-AC5D-987046FDB574} iPodManagerUI Class  
 Thu Jan 7 22:11:06 2016 Z

## SOFTWARE OUTPUT

```

{24CD4DE9-FF84-4701-9DC1-9B69E0D1090A} DNSSDService Class
{5E93C5A9-7516-4259-A67B-41A656F6E01C} DNSSDRecord Class
{7FD72324-63E1-45AD-B337-4D525BD98DAD} PSFactoryBuffer
{AFEE063C-05BA-4248-A26E-168477F49734} TXTRecord Class
{BEEB932A-8D4A-4619-AEFE-A836F988B221} DNSSDEventManager Class
Thu Dec 17 13:00:43 2015 Z
{BE5018C3-A638-40C1-B4DA-1BE1448353B8}
Sun Dec 6 01:16:55 2015 Z
{62B032B7-F027-4274-BFB1-A0418EB9D0D9}
Sun Dec 6 01:16:54 2015 Z
{F6F571E3-B4D3-45BA-B8AF-2953CFF41189} PSFactoryBuffer
Fri Oct 2 14:25:12 2015 Z
{abcdca3b-de6b-5a7c-b132-6d7cba63e5c5} McIdleTaskAgent Class
{abceca3b-ea5a-496b-a021-5c6bab365e5c} McAMTaskAgent Class
Thu Sep 24 18:59:55 2015 Z
{34C445BA-07EB-4b5d-8EE9-F66BB9DA403B} MtpUsbscanTransport Class
{AAAE762B-A6A2-4c45-B5D8-9A83AFB6BB70} WpdMtpDriver Class
{F1AAAA76-BD01-42e1-A6C0-34FA86ACBB90} WindowsMtp Class
Wed Sep 23 14:00:34 2015 Z
{1705F4AB-AF4A-41dc-9FF5-D774C4987E0E} Custom Video setting Page
{755742BA-C3AD-450a-BF7B-8E4F9D20A830} WDM Custom ICustomCamera Interface
handler
{BF9783AD-5FE4-4e1f-A31E-34F71B8FB2A2} Custom Special Effect Page
Mon Sep 21 00:23:57 2015 Z
{FA8A2DAF-0603-4D2C-AB34-FAB373B571DC} CoPDFXCviewMgr Class
Mon Sep 21 00:23:54 2015 Z
{C7F70A09-F3F8-4344-A688-6BC747A694B6} PSFactoryBuffer
{D584CD7A-B8AF-48f7-A543-45021D439A74} PDF-XChange Viewer ActiveX Arguments
{DFC89414-E8E7-49c0-B14E-EB61245D3A5D} PDF-XChange Viewer Simple ActiveX
{FE36F0F3-F082-41B7-9EED-772505A7C054} PDF-XChange Viewer ActiveX Control
Thu Sep 17 10:02:42 2015 Z
{61095308-52CE-433B-9A66-57B9E5835B60}
Thu Sep 17 10:02:41 2015 Z
{21CB022B-12DA-4981-97DF-6CDCA8615A05} PSFactoryBuffer
Wed Sep 16 04:56:07 2015 Z
{475D0CC9-9014-4EEC-BBE0-905315E7C7FE} scanner Class
{8D3B9A44-D0D8-47C5-A95A-4FCE53850572} HPWia2DriverRoot Class
Sat Sep 12 13:14:58 2015 Z
{BEBA2AA5-B5A7-4DD3-9AD6-43B24CDD3B7D} GWX
{C74C5910-D594-43DD-850F-3AFFEB9B756D} GWX
Sat Sep 12 00:14:20 2015 Z
{59856830-3ECB-4D29-9CFE-DDD0F74B96A2}
{F4E1E7F6-A035-41B3-9856-A3C3A1C4684F} WCF/COM+ Integration Service Moniker 40
Sat Sep 12 00:14:19 2015 Z
{4E9963B7-B2BF-4685-9378-8FEBEA364EF8} Microsoft.AspNet.Snapin.About
{5437FDFA-9EC9-4CCC-8531-42F8D9C19AF7}
Microsoft.AspNet.Snapin.AspNetManagementUtility.4
Fri Sep 11 17:57:57 2015 Z

```

## SOFTWARE OUTPUT

```

{12E6A993-AE52-4F99-8B89-41F985E6C952} Connect Class
Fri Sep 11 17:56:12 2015 Z
{D9E904CA-8865-42E7-B0F0-B7B8C4D54D70} CourierUpTime Class
Fri Sep 11 17:56:11 2015 Z
{6812639B-FD61-4329-9901-22CFDBD690FE} APSNotificationServer Class
{fdd068c2-d51a-4175-8a20-5cbc704ea3bd} NotificationCenter Class
Fri Sep 11 14:56:31 2015 Z
{93821D1D-1047-4239-AA97-40E028199390} PSFactoryBuffer
{AF8B3E35-A68A-4788-BDDA-76D8AE1C4064}
Thu Sep 10 21:48:07 2015 Z
{07B0E5E9-D635-4CD3-B98D-7C10E700DEA0} PimcSurrogate Class
{2A7B042D-578A-4366-9A3D-154C0498458E}
System.Management.Instrumentation.ManagedCommonProvider
{AF44BF80-36DD-4118-B4CF-8B1E3F4FB9CE} PSFactoryBuffer
{BFFECCA7-4069-49F9-B5AB-7CCBB078ED91}
System.ServiceModel.Internal.TransactionBridge
{E23B1CED-5E47-4FDB-AF66-B20370261B5E} PimcManager Class
Thu Sep 10 21:48:06 2015 Z
{45FB4600-E6E8-4928-B25E-50476FF79425} Com Call Wrapper Unmarshal Class 4.0
Thu Sep 10 21:28:36 2015 Z
{0006F063-0000-0000-C000-000000000046}
{0006F069-0000-0000-C000-000000000046}
{0468C085-CA5B-11D0-AF08-00609797F0E0}
{138508bc-1e03-49ea-9c8f-ea9e1d05d65d} @C:\Program Files\Microsoft
Office\Office14\MAPISELL.DLL, -110
{261B8CA9-3BAF-4BD0-B0C2-BF04286785C6}
{34CEAC8D-CBC0-4f77-B7B1-8A60CB6DA0F7} Open Document Format ODT Persistent
Handler
{3B224B11-9363-407e-850F-C9E1FFACD8FB} Zip Persistent Handler
{3DDEB7A4-8ABF-4D82-B9EE-E1F4552E95BE} Open Document Format ODS Persistent
Handler
{435fdbba0-964c-43a7-8aff-cc94e21b2249} Outlook MAPI Mail Previewer
{942f72e2-b5ce-4e6c-8d76-0519b3f1bfff} PSFactoryBuffer
{B4132098-7A03-423D-9463-163CB07C151F} Office Open XML Format Excel Persistent
Handler
{E2F83EED-62DE-4A9F-9CD0-A1D40DCD13B6} Open Document Format ODP Persistent
Handler
{e565b713-6e44-4c9d-8d01-ed208f88879} Outlook Out Of Proc Mapi Handler
{f64b4d4f-5196-4be6-ba86-ab6969c7608f} PSFactoryBuffer
Thu Sep 10 21:28:35 2015 Z
{0002E101-0000-0000-C000-000000000046}
{0002E119-0000-0000-C000-000000000046}
{0002E132-0000-0000-C000-000000000046}
{0002E169-0000-0000-C000-000000000046}
{0002E170-0000-0000-C000-000000000046}
{0002E174-0000-0000-C000-000000000046}
{0002E178-0000-0000-C000-000000000046}
{0002E17C-0000-0000-C000-000000000046}

```

## SOFTWARE OUTPUT

```

{0002E185-0000-0000-C000-000000000046}
{0002E187-0000-0000-C000-000000000046}
{0002E18B-0000-0000-C000-000000000046}
{0006F023-0000-0000-C000-000000000046}
{0006F024-0000-0000-C000-000000000046}
{0006F03A-0000-0000-C000-000000000046}
{0006F045-0000-0000-C000-000000000046}
{0006F04A-0000-0000-C000-000000000046}
{0006F04B-0000-0000-C000-000000000046}
{0006F04C-0000-0000-C000-000000000046}
{0006F04D-0000-0000-C000-000000000046}
{0006F04E-0000-0000-C000-000000000046}
{0006F04F-0000-0000-C000-000000000046}
{0006F050-0000-0000-C000-000000000046}
{0006F051-0000-0000-C000-000000000046}
{0006F053-0000-0000-C000-000000000046}
{0006F054-0000-0000-C000-000000000046}
{0006F055-0000-0000-C000-000000000046}
{0006F056-0000-0000-C000-000000000046}
{0006F057-0000-0000-C000-000000000046}
{0006F058-0000-0000-C000-000000000046}
{0006F059-0000-0000-C000-000000000046}
{0006F067-0000-0000-C000-000000000046}
{0006F068-0000-0000-C000-000000000046}
{000CDB0D-0000-0000-C000-000000000046}
{02BCC737-B171-4746-94C9-0D8A0B2C0089} Microsoft Office Template and Media
Control
{1C3B4210-F441-11CE-B9EA-00AA006B1A69}
{20E823C2-62F3-4638-96BD-90F4F6784EBC} Zip Filter
{274C2936-A842-45f3-A457-FB4BA4ED1BA2} VSTO Controller
{312AB530-ECC9-496E-AE0E-C9E6C5392499} Office Open XML Format Excel Filter
{3133A7FE-BC5F-4D81-BF02-184ECC88D66E} VSTO SmartTag Recognizer
{32CDF9E0-1602-11CE-BFDC-08002B2B8CDA}
{34bb52b0-e577-4285-a0ac-1a9b0eabfe9d} MAPI Shell Context Menu
{367E582C-F71C-4BF9-AA1B-9F62B793E9C5}
{3CA78EDC-E48A-4A21-9562-9245BF90CE3F} Enterprise Projects
{4693FF15-B962-420A-9E5D-176F7D4B8321} Open Document Format ODP Filter
{4C599241-6926-101B-9992-00000B65C6F9}
{4E3C66D5-58D4-491E-A7D4-64AF99AF6E8B} VSTO Loader
{5CEF5610-713D-11CE-80C9-00AA00611080}
{64654B35-A024-4807-89D3-C6FDB5A260C7} VSTO FormRegionsHostX
{6F3DD387-5AF2-492B-BDE2-30FF2F451241}
{760681E7-B985-41CE-BCBE-2985A1DFC61C} VSTO Assembly100
{7CCA70DB-DE7A-4FB7-9B2B-52E2335A3B5A} Enterprise Projects
{805B7F91-C9CF-4EDF-ACA6-775664FDFB3E}
{807573E5-5146-11D5-A672-00B0D022E945} Microsoft Office InfoPath XML Mime Filter
{82B02373-B5BC-11CF-810F-00A0C9030074}
{82B02374-B5BC-11CF-810F-00A0C9030074}

```

## SOFTWARE OUTPUT

```

{82B02375-B5BC-11CF-810F-00A0C9030074}
{83081C08-382C-4ED4-ACCF-DCBECA021010} VSTO Accessor class
{8A683C92-BA84-11CF-8110-00A0C9030074}
{8A683C93-BA84-11CF-8110-00A0C9030074}
{8D4F994C-EBBE-4F8D-BA4B-AE20CD36E72D}
{909E0AE0-16DC-11CE-9E98-00AA00574A4F}
{95F35795-64B1-495D-9DE7-390EECC31EC0} Microsoft Office Project.Task Launch
Control
{97A2762C-403C-4953-A121-7A75ABCE4373}
{99D651D7-5F7C-470E-8A3B-774D5D9536AC} VSTOAddinLoader
{99E0D1EC-0A0D-4E50-B8A1-82A8B6ECE5CB} VSTO SmartTag Action
{9E390D9E-7641-4819-BF38-8EEE08964681} Office SPP WMI Provider
{9FBC2D8F-6F52-4CFA-A86F-096F3E9EB4B2} Open Document Format ODT Filter
{A1EB89D6-0A9C-4575-A0AE-654A990A454C}
{A249E9F6-5B28-4ED1-8AF0-C9B9C5195486} Panelocator Class
{A37BBB42-E8C1-4E09-B9CA-F009CE620C08} VSTO WinFormsHost Control
{AFC20920-DA4E-11CE-B943-00AA006887B4}
{B7EFF951-E52F-45CC-9EF7-57124F2177CC} SmartDocument Class
{BE39F3D6-1B13-11D0-887F-00A0C90F2744}
{BE39F3D7-1B13-11D0-887F-00A0C90F2744}
{BE39F3D8-1B13-11D0-887F-00A0C90F2744}
{BE39F3DA-1B13-11D0-887F-00A0C90F2744}
{C514A18E-862A-45d3-8A5E-62CF54D912B6} Microsoft Office 14 Authorization Control
{CB3F7806-3CB4-409C-BA3B-12D642BE371A} Launcher
{CD7791B9-43FD-42C5-AE42-8DD2811F0419}
{D0B22D03-D05D-4C6D-8AB7-9392E84A87B9}
{D5EC4D34-77DA-4F7A-B8C4-8A910C1C1CFE}
{D9160E22-BDF3-4D8A-818C-D99D10EC7BEF} OSppWmiTokenActivationSigner
{DA936B63-AC8B-11D1-B6E5-00A0C90F2744}
{E2F5480E-ED5A-4DDE-B8A8-F9F297479F62} Open Document Format ODS Filter
{EC04D82C-AA59-4ba4-96B1-27BE3FF05E00} VSTO Mime Handler
{F09D237B-3FD1-4900-BEF2-3471CA68142D} VSTO CTPHostX
Thu Sep 10 21:28:34 2015 Z
{B4F3A835-0E21-4959-BA22-42B3008E02FF} Office Document Cache Handler
Thu Sep 10 20:51:18 2015 Z
{336000AA-AA9A-4988-B1D7-15F64E25182E} PSFactoryBuffer
{5D52C3ED-4D79-4069-82B7-FBD600FC64B7} PSFactoryBuffer
{f4ba59cc-2506-45ae-84c8-78ea8d7f9b3e} Compat Inventory WMI provider
Thu Sep 10 19:54:05 2015 Z
{506F4668-F13E-4AA1-BB04-B43203AB3CC0} ImageExtractorShellExt Class
{8DE0A0A1-96D0-4B04-8EC6-2DBF9BD888DC} QuickViewShellExt Class
{A394DCA9-3727-11D4-BD85-00C04F6B93A4} CVisioFileFilter Class
{D66DC78C-4F61-447F-942B-3FB6980118CF} CInfoTipShellExt Class
{F5BF6FE9-913F-4117-94C7-5040C7E3A6C1} IconHandlerShellExt Class
Thu Sep 10 19:54:03 2015 Z
{993BE281-6695-4BA5-8A2A-7AACBFAAB69E} Microsoft Office Metadata Handler
{C41662BB-1FA0-4CE0-8DC5-9B7F8279FF97} Microsoft Office Thumbnail Handler
Thu Sep 10 19:54:02 2015 Z

```



## SOFTWARE OUTPUT

```

{AB968F1E-E20B-403A-9EB8-72EB0EB6797E}
Thu Sep 10 19:54:01 2015 Z
{4039B326-9F27-4B4A-B460-47A0C6A39D5C} Office Outlook MSG IFilter
{5A98B233-3C59-4B31-944C-0E560D85E6C3} Office Open XML Format Word Filter
{DDFE337F-4987-4EC8-BDE3-133FA63D5D85} Office Open XML Format PowerPoint Filter
{F90DFE0C-CBDF-41FF-8598-EDD8F222A2C8} Office Open XML Format Excel Filter
Thu Sep 10 19:53:58 2015 Z
{4887767F-7ADC-4983-B576-88FB643D6F79} Office Open XML Format Excel Persistent
Handler
{4F46F75F-199F-4C63-8B7D-86D48FE7970C} Office Open XML Format PowerPoint
Persistent Handler
{D3B41FA1-01E3-49AF-AA25-1D0D824275AE} Office Open XML Format Word Persistent
Handler
{FB10BD80-A331-4e9e-9EB7-00279903AD99} Office Outlook MSG Persistent Handler
Thu Sep 10 19:07:29 2015 Z
{B41DB860-64E4-11D2-9906-E49FADC173CA} WinRAR
Thu Sep 10 17:13:12 2015 Z
{0C146D72-9229-49D8-B2C9-D805EF5C69A9} PSFactoryBuffer
{16453650-8364-4e9c-B891-1CF822B38F2E} McAfee MCODS Shim
{89129896-0240-4245-A9F0-866E06263A0D} McAfee McQuarantine Shim
{9d0f8731-12bb-42da-9a27-2f97b8c99998} McAfee VirusScan Recent Events and Logs
Provider
{9EA1A0AD-B6AA-4f94-849C-02C8223CE619} McAfee McRealtimeScan Shim
{A10DDD46-26AA-4b27-8FD1-D8A27A8AAF8C} McAfee McTrustedItem Shim
{DE4F5EAE-49F5-BEED-DA6F-A387DE19EAF4} McAfee RtsExclusions Shim
Thu Sep 10 17:13:11 2015 Z
{874f654b-c2a6-4f89-9195-6c6c3eeb779a} McAfee VirusScan Application Information
Thu Sep 10 17:13:10 2015 Z
{33264B15-ECBD-4191-87A7-6B6422CB3A54} PSFactoryBuffer
{3EF62937-0A7B-4f6c-988D-994620390A80} McAfee VirusScan Engine
Thu Sep 10 17:13:09 2015 Z
{2813D8F5-E8CC-4102-B76A-472A0DF23E51} McVSVr Class
{94478404-6236-40C4-8850-DF09CE6D95BC} PSFactoryBuffer
{D1646887-73BC-429E-A2D3-2299B684F91F} McAfee VSO Setting Manger
{F80EAA49-6471-40B8-84F5-E1C1E4F5644A} EscnPlug
Thu Sep 10 17:09:46 2015 Z
{0CB58125-ED4E-4125-B72E-BA3435AC4421} PSFactoryBuffer
{0EBBBE48-BAD4-4B4C-8E5A-516ABECAE064} McAfee SiteAdvisor Toolbar
{21CBFEC0-E728-420C-B4A4-A58AD2089ABA} McAfee SiteAdvisor saUpKeep
{5513F07E-936B-4E52-9B00-067394E91CC5} McAfee SACore Protocol Handler
{B164E929-A1B6-4A06-B104-2CD0E90A88FF} McAfee SiteAdvisor BHO
Thu Sep 10 17:09:37 2015 Z
{E0EA5F46-A285-4ebd-9AA9-0CD334F5A9C5} MSK OEMConfig
Thu Sep 10 17:09:34 2015 Z
{CF1B3E19-651E-4406-852B-9B7C4BABC82E} PSFactoryBuffer
Thu Sep 10 17:09:33 2015 Z
{60CCDA22-6301-439F-897B-08806DA744F2} PSFactoryBuffer
{F33B322A-8757-4E91-ACE3-28FE07AF968E} PSFactoryBuffer

```

## SOFTWARE OUTPUT

Thu Sep 10 17:09:28 2015 Z  
 {89B3DCD8-9450-49DA-BFA4-7F9A6ED3B9A5} PSFactoryBuffer

Thu Sep 10 17:09:12 2015 Z  
 {4F8C7A2C-C891-400C-B4D7-A04D08CEF024} PSFactoryBuffer  
 {E0827905-82D3-4566-ABA1-C67E4447F27E} PSFactoryBuffer

Thu Sep 10 17:09:09 2015 Z  
 {A404171B-F5E6-40F5-8E35-90C616052B28} PSFactoryBuffer  
 {D38B2A0A-D751-4795-8CAC-DBCE8EF7D103} PSFactoryBuffer

Thu Sep 10 17:09:08 2015 Z  
 {2C026D52-3200-44EF-A616-C6437A53AE45} PSFactoryBuffer  
 {4D13AE0B-CCCE-49AC-BB17-7BC48DDD7AA8} PSFactoryBuffer  
 {80AD3138-435C-499B-A71F-7F129960E6F7} PSFactoryBuffer

Thu Sep 10 17:09:06 2015 Z  
 {16D2A02D-7200-4AD7-97FA-BEEE9D3AF9FC} PSFactoryBuffer  
 {5C95C8F6-B4B4-47E7-9241-ECB5FA0A2C91} PSFactoryBuffer  
 {6C92090B-807D-4473-8607-27A4449BFA74} PSFactoryBuffer  
 {95159ED8-48A3-4E84-9C75-550675F1F47F} PSFactoryBuffer

Thu Sep 10 17:09:05 2015 Z  
 {11B6414A-7285-46BA-968E-1AD21C982109} McAfee Event Registration  
 {26016851-6AB3-449C-917F-198A8FB4FAE3} McAfee Event Broker  
 {683C7EA1-3A4B-4764-A8E6-768C4F38BBA6} PSFactoryBuffer  
 {9EFCE8D1-F3E0-460E-B301-0C08C95C1843} PSFactoryBuffer  
 {DB112051-BFD7-4D32-AD3B-DF797F55A870} McAfee Version

Thu Sep 10 17:07:34 2015 Z  
 {0A9B27F1-F902-43a1-8663-BFF940E2F280} RedirVer Class  
 {0E3F1A07-DA76-4168-BA0F-4AFA3007CEFF} EmProxyVer Class  
 {858CCFAD-107A-4806-ACC4-68C84614EDDE} McSvcSubsystem Class  
 {D578D806-C260-4321-9AE0-3B181B39538C} ProxyVer Class

Thu Sep 10 17:07:27 2015 Z  
 {C8C3A940-EE0E-4BFD-A151-E31A7F05F866} PSFactoryBuffer

Thu Sep 10 17:07:21 2015 Z  
 {590AB12E-F706-4BA8-9D08-A1EEC69A687D} PSFactoryBuffer

Thu Sep 10 16:40:57 2015 Z  
 {A2970C7C-8392-4E6F-8B51-B763CF38E13C}

Thu Sep 10 16:32:34 2015 Z  
 {1F2FD001-0148-474e-843E-D6D37A848D62} Microsoft Office OneNote Windows Desktop

Search IFilter Base Class ID  
 {42042206-2D85-11D3-8CFF-005004838597}  
 {6D01EC38-83F9-45df-99F0-8A880993928D} Microsoft Office OneNote Windows Desktop

Search IFilter  
 {72773E1A-B711-4d8d-81FA-B9A43B0650DD} Microsoft Office OneNote Windows Desktop

Search IFilter Persistent handler  
 {807563E5-5146-11D5-A672-00B0D022E945} Microsoft Office InfoPath XML Mime Filter  
 {88D969E5-F192-11D4-A65F-0040963251E5} XML DOM Document 5.0  
 {88D969E6-F192-11D4-A65F-0040963251E5} Free Threaded XML DOM Document 5.0  
 {88D969E7-F192-11D4-A65F-0040963251E5} XML Schema Cache 5.0  
 {88D969E8-F192-11D4-A65F-0040963251E5} XSL Template 5.0  
 {88D969E9-F192-11D4-A65F-0040963251E5} XML Data Source Object 5.0

## SOFTWARE OUTPUT

```

{88D969EA-F192-11D4-A65F-0040963251E5} XML HTTP 5.0
{88D969EB-F192-11D4-A65F-0040963251E5} Server XML HTTP 5.0
{88D969EC-8B8B-4C3D-859E-AF6CD158BE0F} SAX XML Reader 5.0
{88D969EE-F192-11D4-A65F-0040963251E5} SAXAttributes 5.0
{88D969EF-F192-11D4-A65F-0040963251E5} MXXMLWriter 5.0
{88D969F0-F192-11D4-A65F-0040963251E5} MXHTMLWriter 5.0
{88D969F1-F192-11D4-A65F-0040963251E5} MXNamespaceManager 5.0
{88D969F5-F192-11D4-A65F-0040963251E5} MXDigitalSignature 5.0
{B8D12492-CE0F-40AD-83EA-099A03D493F1} Microsoft Office OneNote Filter
{E772CEB3-E203-4828-ADF1-765713D981B8} Microsoft Office OneNote Section
persistent handler
{EDA26AA4-13EE-4304-8115-F7A5AE41D72F} Microsoft Office OneNote Windows Desktop
Search Protocol Handler
Fri Feb 20 18:22:43 2015 Z
{0F195FA1-CCF0-11D2-8B20-00A0C93CB1F4} CUIService Class
{3AB1675A-CCFF-11D2-8B20-00A0C93CB1F4} GraphicsShellExt Class
{9CEE304E-DC6C-11D2-B561-00A0C92E6848} CUIDriver Class
{D4FA3D4E-BE69-11D4-AA30-00902704C6BF} DataObject Class
{FC03875E-6012-4349-B5C5-C42E9FE26AD2} CloneViewHelper Class
Fri Feb 20 16:54:08 2015 Z
{2FAF63B8-11DB-4E13-91C0-A99866F6BC9B} DelayAPOGFX Class
Fri Feb 20 16:53:55 2015 Z
{0E799A91-CDDC-471B-A803-2DB82FAFB726} AMD Playback Decoder MFT
{17796aeb-0f66-4663-b8fb-99cbee0224ce} AMD D3D11 Hardware MFT Playback Decoder
{8C00C8CE-A6BA-442F-9185-2D68E4FCA8EB} AMD Fast (DnD) Decoder
{EBB5845F-CA80-11CF-BD3C-008029E89281}
Mon Dec 1 14:16:44 2014 Z
{F02602C4-3C2A-473B-B35E-679A0076A4A5} WatAdminSvcObject Class
{F1CA3CE9-57E0-4862-B35F-C55328F05F1C} Windows Activation Technologies ActiveX
Control
Mon Dec 1 14:13:54 2014 Z
{0002DF01-0000-0000-C000-000000000046} Internet Explorer(Ver 1.0)
{00C429C0-0BA9-11d2-A484-00C04F8EFB69} CrBlinds
{0358b920-0ac7-461f-98f4-58e32cd89148} Wininet Cache task object
{049F2CE6-D996-4721-897A-DB15CE9EB73D} Iris
{057EEE47-2572-4AA1-88D7-60CE2149E33C} PSFactoryBuffer
{05BDC38E-5493-487a-A7FF-8CF2246ABC13} IE Background Task Scheduler
{05f6fe1a-ecef-11d0-aae7-00c04fc9b304} IntDitherer Class
{06EEE834-461C-42c2-8DCF-1502B527B1F9} URL Shortcut PropSetStorage Mapping
{07C45BB1-4A8C-4642-A1F5-237E7215FF66} IE Microsoft BrowserBand
{08165EA0-E946-11CF-9C87-00AA005127ED} WebCheckWebCrawler
{0968e258-16c7-4dba-aa86-462dd61e31a3} PersistentZoneIdentifier
{098870b6-39ea-480b-b8b5-dd0167c4db59} IE OpenService Manager
{0b6d74fe-ad29-4c92-ac06-f06bc2f238a7} Microsoft Feeds Request
{0BE9F729-A4E0-4BED-9FB3-85F1858143B7} SSPWorkspace Class
{0C7EFBDE-0303-4c6f-A4F7-31FA2BE5E397} AlphaImageLoader
{0E890F83-5F79-11D1-9043-00C04FD9189D} DXSurface
{10BCEB99-FAAC-4080-B2FA-D07CD671EEF2} IE Recovery Store

```

## SOFTWARE OUTPUT

{11016101-E366-4D22-BC06-4ADA335C892B} IE History and Feeds Shell Data Source for Windows Search

{164484A9-35D9-4FB7-9FAB-48273B96AA1D} RadialWipe

{16B280C5-EE70-11D1-9066-00C04FD9189D} Fade

{16B280C8-EE70-11D1-9066-00C04FD9189D} BasicImage

{16d51579-a30b-4c8b-a276-0ff4dc41e755} JScript Language

{181D6C15-60A6-4BC7-A8E7-389D5BFE4841} Reading Mode Viewer

{182C3813-DF97-40fa-9C4E-B7D3E74F00CA} Pinned Site Shortcut

{18845040-0fa5-11d1-ba19-00c04fd912d0} Microsoft HTML Load Options

{19916E01-B44E-4e31-94A4-4696DF46157B} InformationCardSignInHelper Class

{1a6fe369-f28c-4ad9-a3e6-2bcb50807cf1} Developer Tools

{1BE75CA5-140F-4FBC-9A99-B522F1A1A30A} RdpEndpoint Class

{1C1EDB47-CE22-4bbb-B608-77B48F83C823} IE Fade Task

{1D1F0730-0748-4b5f-81DF-865694BD07AC} IE OrderListExport

{1E54333B-2A00-11d1-8198-0000F87557DB} DXLUTBuilder

{205D7A97-F16D-4691-86EF-F3075DCCA57D} IE Menu Desk Bar

{20CCEF1E-0185-41a5-A933-509C43B54F98} ShdocvwBroker

{2183DACA-D0BF-4a31-97F7-B87618A81955} IE Shared Task Scheduler

{23E26328-3928-40F2-95E5-93CAD69016EB} ZigZag

{25336920-03F9-11CF-8FD0-00AA00686F13} HTML Document

{25336921-03F9-11CF-8FD0-00AA00686F13} Microsoft HTML Document 6.0

{28BCCB9A-E66B-463C-82A4-09F320DE94D7} F12 Developer Tools

{2B4F54B1-3D6D-11d0-8258-00C04FD5AE38} Shell BindStatusCallback Proxy

{2BC0EF29-E6BA-11d1-81DD-0000F87557DB} Convolution

{2E7700B7-27C4-437F-9FBF-1E8BE2817566} RandomBars

{301B94BA-5D25-4A12-BFFE-3B6E7A616585} Microsoft RDP Client Control

(redistributable) - version 10

{3028902F-6374-48b2-8DC6-9725E775B926} IE AutoComplete

{3050F391-98B5-11CF-BB82-00AA00BDCE0B} Microsoft HTML Window Security Proxy

{3050F3B2-98B5-11CF-BB82-00AA00BDCE0B} Microsoft HTML Javascript Pluggable

Protocol

{3050f3B3-98b5-11cf-bb82-00aa00bdce0b} %Microsoft Image Element Browse Property

Page%

{3050f3B4-98b5-11cf-bb82-00aa00bdce0b} %Microsoft Document Browse Property Page%

{3050f3BB-98b5-11cf-bb82-00aa00bdce0b} %Microsoft Anchor Element Browse Property

Page%

{3050F3BC-98B5-11CF-BB82-00AA00BDCE0B} Microsoft HTML Resource Pluggable Protocol

{3050F3C2-98B5-11CF-BB82-00AA00BDCE0B} Microsoft HTML DwnBindInfo

{3050F3D6-98B5-11CF-BB82-00AA00BDCE0B} IImgCtx

{3050F3D9-98B5-11CF-BB82-00AA00BDCE0B} MHTML Document

{3050f3DA-98B5-11CF-BB82-00AA00BDCE0B} Microsoft HTML Mailto Pluggable Protocol

{3050F406-98B5-11CF-BB82-00AA00BDCE0B} Microsoft HTML About Pluggable Protocol

{3050f499-98b5-11cf-bb82-00aa00bdce0b} Microsoft HTML Recalc

{3050F4CF-98B5-11CF-BB82-00AA00BDCE0B} PeerFactory Class

{3050f4d8-98B5-11CF-BB82-00AA00BDCE0B} HTML Application

{3050f4e1-98b5-11cf-bb82-00aa00bdce0b} HtmlDlgHelper Class

{3050f4f5-98B5-11CF-BB82-00AA00BDCE0B} Trident HTML Editor

{3050f4f8-98b5-11cf-bb82-00aa00bdce0b} Microsoft Html Component

## SOFTWARE OUTPUT

{3050f5be-98b5-11cf-bb82-00aa00bdce0b} DownloadBehavior Class  
 {3050F5C8-98B5-11CF-BB82-00AA00BDCE0B} Microsoft HTA Document 6.0  
 {3050f664-98b5-11cf-bb82-00aa00bdce0b} LayoutRect Class  
 {3050f667-98b5-11cf-bb82-00aa00bdce0b} Microsoft Html Popup Window  
 {3050f67D-98b5-11cf-bb82-00aa00bdce0b} Microsoft Html Document for Popup Window  
 {3050f6b3-98b5-11cf-bb82-00aa00bdce0b} Template Printer class  
 {3050f6cd-98b5-11cf-bb82-00aa00bdce0b} HeaderFooter class  
 {3050f6d4-98b5-11cf-bb82-00aa00bdce0b} DeviceRect Class  
 {3050f819-98b5-11cf-bb82-00aa00bdce0b} HtmlDlgSafeHelper Class  
 {30510483-98B5-11CF-BB82-00AA00BDCE0B} Microsoft HTML Element Context Stream  
 {30590066-98b5-11cf-bb82-00aa00bdce0b} SVG Document  
 {30590067-98b5-11cf-bb82-00aa00bdce0b} XHTML Document  
 {30C3B080-30FB-11d0-B724-00AA006C1A01} CoMapMIMEToCLSID Class  
 {32374F0E-85D3-4408-9BD0-887E3EEAE7F0} IE JScript Profiler Core  
 {32B533BB-EDAE-11d0-BD5A-00AA00B92AF1} AP Class Install Handler filter  
 {333C7BC4-460F-11D0-BC04-0080C7055A83} Tabular Data Control  
 {33F3C8F8-27A1-4DF3-A525-E89CB18881A5} Workspace Setup Discovery Page  
 {34a13fc7-86ab-42e6-a32c-b50666f04ff9} JScript Language Authoring  
 {34a3d570-67d9-4265-a9ee-8c3fa3dfeccf} TravelLog  
 {34e6abfe-e9f4-4ddf-895a-7350e198f26e} Microsoft Feeds Arbiter LoRi Broker  
 {374CEDE0-873A-4C4F-BC86-BCC8CF5116A3} IE HomePageSetting  
 {385A91BC-1E8A-4e4a-A7A6-F4FC1E6CA1BD} DXTFilter  
 {3A04D93B-1EDD-4f3f-A375-A03EC19572C4} MaskFilter  
 {3BC4EE9F-1FC1-44DB-81FA-AD94DEC7AF30} CLSID\_AppRep  
 {3C374A40-BAE4-11CF-BF7D-00AA006946EE} Microsoft Url History Service  
 {3CB169B3-17D9-4E47-8B93-2878998F69A2} WebBrowserHandler Proxy  
 {3DC7A020-0ACD-11CF-A9BB-00AA004AE837} The Internet  
 {3dd53d40-7b8b-11D0-b013-00aa0059ce02} CDL: Asynchronous Pluggable Protocol  
 Handler  
 {3E669F1D-9C23-11d1-9053-00C04FD9189D} DXSurface Modifier  
 {3e71f26d-136f-4545-813f-35276024b705} XML Feed Subscribe Dialog  
 {3F4DACA4-160D-11D2-A8E9-00104B365C9F} VBScript Regular Expression  
 {3F69F351-0379-11D2-A484-00C04F8EFB69} CrIris  
 {421516C1-3CF8-11D2-952A-00C04FA34F05} Chroma  
 {424B71AF-0695-11D2-A484-00C04F8EFB69} CrRadialWipe  
 {429AF92C-A51F-11d2-861E-00C04FA35C89} %Trident API%  
 {4356b08e-ecb5-43d1-8e9f-7bef4fc960fe} Manage Add-ons Admin Broker  
 {43886CD5-6529-41c4-A707-7B3C92C05E68} IE Navigation Bar  
 {43A8F463-4222-11d2-B641-006097DF5BD4} Shell Name Space ListView  
 {447EDBE5-0080-4036-A0BB-7B84C58C604F} IEDataObjectWrapper  
 {44C76ECD-F7FA-411c-9929-1B77BA77F524} IE Menu Site  
 {46CB32FA-B5CA-8A3A-62CA-A7023C0496C5} CIEContentAdvisorBroker  
 {473AA80B-4577-11D1-81A8-0000F87557DB} DX2D Anti-Aliasing  
 {4A03DCB9-6E17-4A39-8845-4EE7DC5331A5} Spiral  
 {4ABF5A06-5568-4834-BEE3-327A6D95A685} Matrix  
 {4b360c3c-d284-4384-abcc-ef133e1445da} CIERegistryHKLMBroker  
 {4B78D326-D922-44f9-AF2A-07805C2A3560} IE Menu Band  
 {4C6470A6-3F91-4f41-850B-DB9BCD074537} Microsoft Feeds Background Sync Component

## SOFTWARE OUTPUT

```

{4CB26C03-FF93-11d0-817E-0000F87557DB} DXTaskManager
{4CCEA634-FBE0-11d1-906A-00C04FD9189D} Pixelate
{4D5C8C2A-D075-11d0-B416-00C04FB90376} Microsoft CommBand
{4DFED3F9-B794-4d3c-973B-DDA1C28105A9} Private Profile Object
{5220cb21-c88d-11cf-b347-00aa00a28331} Microsoft Licensed Class Manager 1.0
{528d46b3-3a4b-4b13-bf74-d9cbd7306e07} XML Feed Document
{53510d24-57eb-4713-9afb-e6e60530b87e} IE RSS Feeds Tasks
{54702535-2606-11D1-999C-0000F8756A10} Text Label Class
{55136805-B2DE-11D1-B9F2-00A0C98BC547} Shell Name Space
{553858A7-4922-4e7e-B1C1-97140C1C16EF} IE Component Categories cache daemon
{555278E2-05DB-11D1-883A-3C8B00C10000} Scale
{55b70dec-4b3b-4e26-ae9c-9e8d131843a1} Microsoft Feeds Background Task Scheduling
{5828227c-20cf-4408-b73f-73ab70b8849f} UMRDPProtocolManager Class
{5AE1DAE0-1461-11d2-A484-00C04F8EFB69} Wheel
{5bbd58bb-993e-4c17-8af6-3af8e908fca8} IE Spelling Dictionary Installer Broker
{5F681803-2900-4C43-A1CC-CF405404A676} Microsoft RDP Client Control
(redistributable) - version 9
{6038EF75-ABFC-4e59-AB6F-12D397F6568D} IE Microsoft History AutoComplete List
{607fd4e8-0a03-11d1-ab1d-00c04fc9b304} CoICOFiler Class
{623E2882-FC0E-11d1-9A77-0000F8756A10} Gradient
{63A4B1FC-259A-4A5B-8129-A83B8C9E6F4F} Strips
{649EEC1E-B579-4E8C-BB3B-4997F8426536} DXTFilerBehavior
{64AB4BB7-111E-11d1-8F79-00C04FC2FBE1} Microsoft Shell UI Helper
{6A01FDA0-30DF-11d0-B724-00AA006C1A01} CoSniffStream Class
{6B4ECC4F-16D1-4474-94AB-5A763F2A54AE} IE Tracking Shell Menu
{6B7F33AC-D91D-4563-BF36-0ACCB24E66FB} MsRdpSessionManagerSingleUse Class
{6CF9B800-50DB-46B5-9218-EACF07F5E414} Internet Explorer ETW Collector Service
{6E449686-C509-11CF-AAFA-00AA00B6015C} Microsoft Active Setup Engine
{6f5bad87-9d5e-459f-bd03-3957407051ca} IEWindows
{7057e952-bd1b-11d1-8919-00c04fc2c836} Microsoft DocHost User Interface Handler
{7312498D-E87A-11d1-81E0-0000F87557DB} Blur
{73CFD649-CD48-4fd8-A272-2070EA56526B} IE BandProxy
{7658F2A2-0A83-11d2-A484-00C04F8EFB69} CrStretch
{766BF2AE-D650-11d1-9811-00C04FC31D2E} HomePage Class
{76F363F2-7E9F-4ED7-A6A7-EE30351B6628} Inset
{79eac9e0-baf9-11ce-8c82-00aa004ba90b} URL Moniker
{79eac9e2-baf9-11ce-8c82-00aa004ba90b} http: Asynchronous Pluggable Protocol
Handler
{79eac9e3-baf9-11ce-8c82-00aa004ba90b} ftp: Asynchronous Pluggable Protocol
Handler
{79eac9e5-baf9-11ce-8c82-00aa004ba90b} https: Asynchronous Pluggable Protocol
Handler
{79eac9e6-baf9-11ce-8c82-00aa004ba90b} mk: Asynchronous Pluggable Protocol Handler
{79eac9e7-baf9-11ce-8c82-00aa004ba90b} file:, local: Asynchronous Pluggable
Protocol Handler
{79EAC9F1-BAF9-11CE-8C82-00AA004BA90B} URLMoniker ProxyStub Factory
{79eac9f2-baf9-11ce-8c82-00aa004ba90b} Async BindCtx
{7AB36653-1796-484B-BDFA-E74F1DB7C1DC} Microsoft Spell Checker Factory Class

```

## SOFTWARE OUTPUT

{7b40792d-05ff-44c4-9058-f440c71f17d4}	Windows trace relogging support.
{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}	Security Manager
{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}	URL Zone Manager
{7BD29E00-76C1-11CF-9DD0-00A0C9034933}	Temporary Internet Files
{7BD29E01-76C1-11CF-9DD0-00A0C9034933}	Temporary Internet Files
{7D559C10-9FE9-11d0-93F7-00AA0059CE02}	Code Download Agent
{7DED4D39-BE20-4AB6-983A-EB4ADCD9C93D}	CLSID_AppRepParm
{7E8BC44E-AEFF-11D1-89C2-00C04FB6BFC4}	
{7EE0A24E-A8C6-46ae-A875-8E7C3D18AEAF}	Favorites IFilter
{7FC0B86E-5FA7-11d1-BC7C-00C04FD929DB}	WebCheck SyncMgr Handler
{810E402F-056B-11D2-A484-00C04F8EFB69}	CrSlide
{81397204-F51A-4571-8D7B-DC030521AABD}	DXTFilterFactory
{8369AB20-56C9-11D0-94E8-00AA0059CE02}	Cleaner for Downloaded Program Files
{842a1268-6e6a-465c-868f-8bc445b9828f}	JScript Language
{8652CE55-9E80-11D1-9053-00C04FD9189D}	DXRasterizer Class
{871C5380-42A0-1069-A2EA-08002B30309D}	
{8856F961-340A-11D0-A96B-00C04FD705A2}	Microsoft Web Browser
{88C6C381-2E85-11D0-94DE-444553540000}	ActiveX Cache Folder
{8A11B5FA-3C92-4E8B-8382-3C71B757D679}	IE RSS Search Protocol Handler
{8B918B82-7985-4C24-89DF-C33AD2BBFBCD}	Microsoft RDP Client Control - version 10
{8c537469-1ea9-4c85-9947-7e418500cdd4}	ProtectedModeAPI
{8CD34779-9F10-4f9b-ADFB-B3FAEABDAB5A}	.url File Persistent Handler
{8E6E6079-0CB7-11d2-8F10-0000F87ABD16}	Offline Pages Cleaner
{8E989135-2736-4767-8160-EA3613F69D24}	IEDropSourceWrapper
{8fe85d00-4647-40b9-87e4-5eb8a52f4759}	Developer Tools
{93073C40-0BA5-11d2-A484-00C04F8EFB69}	CrInset
{93852550-5403-4E1B-AF8C-5806F151B2F5}	JScript Debugger IDE
{94C00EC1-6E51-447A-87FA-8DF83767C155}	JScript Diagnostic Component
{98FF6D4B-6387-4b0a-8FBD-C5C4BB17B4F8}	IE MRU AutoComplete List
{9a096bb5-9dc3-4d1c-8526-c3cbf991ea4e}	IE RSS Feeds Folder
{9A43A844-0831-11D1-817F-0000F87557DB}	Compositor
{9A4A4A51-FB3A-4F4B-9B57-A2912A289769}	Blinds
{9B0EFD60-F7B0-11D0-BAEF-00C04FC308C9}	Temporary Internet Files Cleaner
{9c7a1728-b694-427a-94a2-a1b2c60f0360}	ShdocvwBroker
{9D958C62-3954-4b44-8FAB-C4670C1DB4C2}	IE Microsoft Shell Folder AutoComplete

List

{9F8E6421-3D9B-11D2-952A-00C04FA34F05}	Glow
{9FAE1230-74AC-4e33-B59C-4051BBEB0803}	IE Thread Handshake
{A1BFB370-5A9F-4429-BB72-B13E2FEAEDEF}	ICMFilter
{A3BC03A0-041D-42E3-AD22-882B7865C9C5}	Microsoft RDP Client Control - version 9
{A3CCEDF7-2DE2-11D0-86F4-00A0C913F750}	CoPNGFilter Class
{A3DD4F92-658A-410F-84FD-6FBBBEF2FFFE}	Internet Options
{A6B222AB-A5EA-4899-B230-084657EDDC7D}	Browser Thread State
{A7256C32-F6C3-4673-82BA-30764F9004DA}	RdpEndpoint Class
{A7C06739-500F-4E8C-99A8-2BD6955899EB}	PSFactoryBuffer
{a7c922a0-a197-4ae4-8fcd-2236bb4cf515}	Microsoft Feeds LoRi Broker
{A7EE7F34-3BD1-427f-9231-F941E9B7E1FE}	DXTFilterCollection
{A860CE50-3910-11d0-86FC-00A0C913F750}	CoDitherToRGB8 Class

## SOFTWARE OUTPUT

```

{AAC2B978-266D-48ae-AA28-60A3EBB872D0} IE RSS FeedFolder Tasks
{ABBE31D0-6DAE-11D0-BECA-00C04FD940BE} Subscription Mgr
{ACA97E00-0C7D-11d2-A484-00C04F8EFB69} CrSpiral
{ACE52D03-E5CD-4b20-82FF-E71B11BEAE1D} Shell Name Space ListView
{ADC6CB82-424C-11D2-952A-00C04FA34F05} Alpha
{ADC6CB86-424C-11D2-952A-00C04FA34F05} DropShadow
{ADC6CB88-424C-11D2-952A-00C04FA34F05} Wave
{AE24FDAE-03C6-11D1-8B76-0080C744F389} Microsoft Scriptlet Component
{AF279B30-86EB-11D1-81BF-0000F87557DB} Wipe
{B15B8DC0-C7E1-11d0-8680-00AA00BDCB71} SoftDist
{B31C5FAE-961F-415b-BAF0-E697A5178B94} IE Microsoft Multiple AutoComplete List
Container
{B3EE7802-8224-4787-A1EA-F0DE16DEABD3} CheckerBoard
{B54F3741-5B07-11cf-A4B0-00AA004A55E8} VB Script Language
{B54F3742-5B07-11cf-A4B0-00AA004A55E8} VB Script Language Authoring
{B54F3743-5B07-11cf-A4B0-00AA004A55E8} VBScript Language Encoding
{B96F67A2-30C2-47E8-BD85-70A2C948B50F} GradientWipe
{bdb57ff2-79b9-4205-9447-f5fe85f37312} Internet Explorer Add-on Installer
{BFAD62EE-9D54-4b2a-BF3B-76F90697BD2A} IE Shell Rebar BandSite
{BFC880F1-7484-11d0-8309-00AA00B6015C} Download Site Manager
{C20ED5C4-0A2E-4F66-9BE2-86A1C823DD68} PSFactoryBuffer
{C21B45B8-5D76-4575-BA27-54823098C491} IE Microsoft Docking Bar Property Bag
{c2c4f00a-720e-4389-aeb9-e9c4b0d93c6f} InformationCardElementBehaviorFactory
Class
{c39ee728-d419-4bd4-a3ef-eda059dbd935} WinInetBroker Class
{C3BDF740-0B58-11d2-A484-00C04F8EFB69} CrBarn
{c5efd803-50f8-43cd-9ab8-aafc1394c9e0} IE OpenService Activity Manager
{C6365470-F667-11d1-9067-00C04FD9189D} Gradient DXSurface
{c6cc0d21-895d-49cc-98f1-d208cd71e047} Internet Explorer Settings Broker
{C8059EB6-D2FC-4ecf-A15F-AF427F5E4DB6} Feeds Background Sync
{CFBFAE00-17A6-11D0-99CB-00C04FD64497} Microsoft Url Search Hook
{D1C5A1E7-CC47-4E32-BDD2-4B3C5FC50AF5} Slide
{D1FE6762-FC48-11D0-883A-3C8B00C10000} DXTransformFactory Class
{D5E8041D-920F-45e9-B8FB-B1DEB82C6E5E}
{d63c23c5-53e6-48d5-adda-a385b6bb9c7b} CIEInetcplRasBroker
{DC651A43-0720-4a2b-9971-BD2EF1329A3D} IE Component Categories conditional cache
daemon
{DD13DE77-D3BA-42D4-B5C6-7745FA4E2D4B} MotionBlur
{DF1E92F3-F333-4EF5-9C38-B75CB65FFC39} Windows.Globalization
{DF2FCE13-25EC-45bb-9D4C-CECD47C2430C} CUri
{E2E760C5-BF0D-4241-BFD6-6D0AAB648AC9} IE WS Change Notify
{E31E87C4-86EA-4940-9B8A-5BD5D179A737} RevealTrans
{E48B2549-D510-4A76-8A5F-FC126A6215F0} CLSID_AntiPhishingBrowserSolution
{E569BDE7-A8DC-47F3-893F-FD2B31B3EEFD} Browser Application State
{E6E73D20-0C8A-11d2-A484-00C04F8EFB69} CrZigzag
{E6EE9AAC-F76B-4947-8260-A9F136138E11} IE Shell Band Site Menu
{E71B4063-3E59-11D2-952A-00C04FA34F05} Shadow
{E7E4BC40-E76A-11CE-A9BB-00AA004AE837} Shell DocObject Viewer

```



## SOFTWARE OUTPUT

```

{EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B} Microsoft Web Browser Version 1
{EC9BA17D-60B5-462B-A6D8-14B89057E22A} Barn
{ed72f0d2-b701-4c53-adc3-f2fb59946dd8} ProtectedModeAPI
{EE0BDDFA-8373-4cc4-85D8-0618E453187C} IE History Search Protocol Handler
{F088DE73-BDD0-4E3C-81F8-6D32F4FE9D28} Stretch
{F2CF5485-4E02-4f68-819C-B92DE9277049} &Links
{F4D36777-EAED-4cc5-9FE7-827BE5190B20} Microsoft Feeds Scheduler
{F515306D-0156-11d2-81EA-0000F87557DB} Emboss
{F515306E-0156-11d2-81EA-0000F87557DB} Engrave
{F5175861-2688-11d0-9C5E-00AA00A45957} Subscription Folder
{F74B1266-FF39-4B62-8B6B-29C09920852C} PSFactoryBuffer
{F7F4A1B6-8E87-452f-A2D7-3077F508DBC0} RandomDissolve
{F83DAC1C-9BB9-4f2b-B619-09819DA81B0E} IE Registry Tree Options Utility
{F9EFBEC2-4302-11D2-952A-00C04FA34F05} Light
{faeb54c4-f66f-4806-83a0-805299f5e3ad} Microsoft Feeds Manager (scripting)
{FBF23B40-E3F0-101B-8488-00AA003E56F8} Internet Shortcut
{FD7F26E3-9788-4070-BEEC-4EAECBCDDA60} IE JScript Profiler Core
{FDE7673D-2E19-4145-8376-BBD58C4BC7BA} IE Custom MRU AutoCompleted List
{FE6B11C3-C72E-4061-86C6-9D163121F229} Microsoft Feeds Manager
{FF393560-C2A7-11CF-BFF4-444553540000} History
{fffd90217-f7c2-4434-9ee1-6f1b530db20f} XML Feed Moniker
Mon Dec 1 14:13:22 2014 Z
{10072CEC-8CC1-11D1-986E-00A0C955B42E} PeerDraw Class
{17FE9752-0B5A-4665-84CD-569794602F5C}
{C5621364-87CC-4731-8947-929CAE75323E} PSFactoryBuffer
{D6FCA954-F7AE-4EAC-8783-85F5E4ABD840} PSFactoryBuffer
{DF4FCC34-067A-4E0A-8352-4A1A5095346E}
{F2C4CDB0-2714-42AD-A948-2ED958A322E3} WorkspaceResTypeRegistry Class
Mon Dec 1 12:59:32 2014 Z
{047ea9a0-93bb-415f-a1c3-d7aeb3dd5087}
Mon Dec 1 12:59:23 2014 Z
{62dc1a93-ae24-464c-a43e-452f824c4250} WM LFX APO
{637c490d-eee3-4c0a-973f-371958802da2} WM GFX APO
Mon Dec 1 12:59:13 2014 Z
{016B931D-8430-4988-8510-C69C214CFF32} Overlay Class
{078AEF33-C48A-49F7-AFF3-A0EE810BFE7C} Settings Class
{12E3793C-7C3C-4C00-BC4E-C79849B3F430} TVParam Class
{27E7234F-429F-4787-AC8F-8AADDED01355} PSFactoryBuffer
{280A8F40-E382-11D2-B561-00A0C92E6848} Software\Intel\Display\igfxcui
{40CB6EA0-AB2A-45F8-BA45-2DC7756A7B49} EDID Class
{4501A903-BF07-11D4-AA30-00902704C6BF} DataObjectInit Class
{6C4BE3D5-831A-42ED-AA62-2AEB34C8CBA4} CloneViewHelper Class
{7160A13D-73DA-4CEA-95B9-37356478588A} CUIExternal Class
{999276E0-DA71-4743-8F02-0AB0A2D65558} MCCS Class
{9B908879-E03F-4D0C-ACB3-9065B1155460} Rotation Class
{A354BD60-4C0A-11d3-B561-00A0C92E6848} DataObject Class
{C071C982-2EB2-4D3A-9821-E4B31B0142C8} Scheme Class
{C2BFE331-6739-4270-86C9-493D9A04CD38} DisplayConfig Class

```

## SOFTWARE OUTPUT

{C332C124-340D-4430-AA0D-C75602876FCC} CUIPower Class  
 {DCB2D492-5F4F-4378-8FF4-DA87062D42E3} OpenGL Class  
 {DDA11344-AB20-4AEC-94C4-6AA091574CD0} PSFactoryBuffer  
 {EE2D6561-D63C-11D2-B561-00A0C92E6848} ShellExt Class  
 {FE9617F6-E606-42AA-BECC-0E9CDA246D63} Color Class  
 Mon Dec 1 12:56:39 2014 Z  
 {0CA545C6-37AD-4A6C-BF92-9F7610067EF5} HNetCfg.FwOpenPort  
 {1fb2a002-4c6c-4de7-85c2-cb8db9a4f728} Microsoft Disk Quota UI Elevation Helper  
 {26D32566-760A-40A2-AA82-A40366528916} WUPublishedAppInstallorElevator Class  
 {2C5BC43E-3369-4C33-AB0C-BE9469677AF4} HNetCfg.FwRule  
 {304CE942-6E39-40D8-943A-B913C40C9CD4} HNetCfg.FwMgr  
 {4026492F-2F69-46B8-B9BF-5654FC07E423} Windows Firewall  
 {78CB147A-98EA-4AA6-B0DF-C8681F69341C} CardSpace  
 {E2B3C97F-6AE1-41AC-817A-F6F92166D7DD} HNetCfg.FwPolicy2  
 {EC9846B3-2762-4A6B-A214-6ACB603462D2} HNetCfg.FwAuthorizedApplication  
 Sat Nov 29 16:11:52 2014 Z  
 {C1A6713B-F5BA-4340-BFE5-07DA0ED49A27} Superseded Updates Cleanup  
 Sat Nov 29 16:07:00 2014 Z  
 {317D06E8-5F24-433D-BDF7-79CE68D8ABC2}  
 {348ef17d-6c81-4982-92b4-ee188a43867a} PrintDocumentPackageTargetFactory  
 {812F944A-C5C8-4CD9-B0A6-B3DA802F228D} UIAnimationTransitionLibrary2  
 {84302F97-7F7B-4040-B190-72AC9D18E420} UIAnimationTransitionFactory2  
 {D25D8842-8884-4A4A-B321-091314379BDD} UIAnimationManager2  
 {E018945B-AA86-4008-9BD4-6777A1E40C11}  
 {E1553E07-5939-4CFD-BE24-3BCEBA2F148C} Proxy CLSID  
 Tue Apr 12 08:28:59 2011 Z  
 {00C6D95F-329C-409a-81D7-C46C66EA7F33} DefaultLocation  
 {010911E2-F61C-479B-B08C-43E6D1299EFE}  
 {01BD2313-DAF5-4e02-AE3F-F66613712278} MCSyncTVPlayer Class  
 {0228576F-6E6C-4E1A-B175-0E46A316AFE2} MediaStatusAggregator Class  
 {0365BE92-BD3F-47f5-8BB6-2EEF7AF5CAE7} SimpleInputItem Class  
 {03A84965-6E86-49C5-B831-826B38732363} PSFactoryBuffer  
 {045EFB3B-3EC4-4D6D-99A5-E87E23AEE929} EHomeC2RDropTarget Class  
 {05376005-47A0-4BDA-8B5F-7EB84D50CFEF} PSFactoryBuffer  
 {054AAE20-4BEA-4347-8A35-64A533254A9D} UIHost Class  
 {05943B92-0930-4129-B689-BC657A94B280} MCMDE RTSP SINK ACTIVATE  
 {069501DC-D776-4778-8C76-81D7A3DFFBB7} TVThumb Class  
 {06DA0625-9701-43da-BFD7-FBEEA2180A1E} HotStart User Agent  
 {07461CC0-878C-4C0F-9255-7DDB269B363B} CHSInputModule Class  
 {075DB5A6-4C67-4816-AE00-7451EC2AAA51} NBDocument Class  
 {07DC68FA-A15D-4E44-93DE-645060C7B469} HandWritingSkinProps Class  
 {09E67AD4-950A-447a-826E-BD5DFCEF5D99} Microsoft Network Tuner Manager  
 {0AEA3667-1039-43ff-8D21-B1A162090671} AppIdPolicyHelper Class  
 {0B3F871D-38D9-4677-8853-A247C6366483} RecoveryTaskDispatchServer Class  
 {0c98b8bc-273c-464d-938a-b9709607e137} Wireless Setup Class  
 {0FDE5092-AA2A-11D1-A7D4-0000F87571E3} Group Policy About Information  
 {11FD394B-6C4C-49d8-9918-7D212CD311CB} GLIDPlugInQAM Class  
 {14834D34-8CEE-459e-8520-2264EC46E099} SharedHWProperties Class

## SOFTWARE OUTPUT

{15D633E2-AD00-465b-9EC7-F56B7CDF8E27} Tablet PC Input Panel  
 {188db6a1-5b9a-489e-bb92-0f900822ac9d} McxRemoteDvrPlayer Class  
 {19371BCB-2BFF-4F74-BB8E-3ABEA71B9E7D} InkWatsonWizard  
 {1AE53973-2F5C-4F9E-9B68-619D309E47A3} GLIDLoaderHandler Class  
 {1B76DD18-2CB4-41A4-BD69-5FB8287F7814}  
 Microsoft.MediaCenter.Internal.LaunchMediaCenter  
 {1BC972D6-555C-4FF7-BE2C-C584021A0A6A} Software installation  
 {1E2D67D6-F596-4640-84F6-CE09D630E983} ShapeCollector Class  
 {21ABC687-760C-41F3-B005-F2C5BA222054} ARIBDCCapture Class  
 {2331D136-E39D-4019-92D6-7CE5579962FB} Sensors Sensor Configuration Helper  
 {23571E11-E545-4DD8-A337-B89BF44B10DF} PSFactoryBuffer  
 {243EDD7B-1ED1-4aa4-974C-0A370DA9DAFA} MCAsyncTVPlayer Class  
 {26fa7c37-2cd3-4897-9499-33330e075cbd} korinputmodule Class  
 {289AE5EE-562C-4350-A8CB-0CB0587A12FF}  
 {2D3AC5E6-D557-42EE-AB8A-F95239E9939F} DiscBurner Class  
 {2DCD1DAF-A110-49c0-BFDB-6FDF557B5FDF} Offline Files WMI Provider  
 {2E1AE5DF-5A6F-420A-9B7B-41E5BA8FA36D} HWProp Class  
 {2E483DC9-7E4D-4861-B496-7E00B7FA184F} NbTextLayoutPageText Class  
 {2EB444B3-0C42-490f-9F28-C77129ACA136} Windows Search Service Media Center  
 Protocol Handler  
 {2F7EE4B6-6FF5-4EB4-B24A-2BFC41117171} Microsoft TV Captions Decoder  
 {2FD934BC-E860-4898-A581-B7C6486CA332} CiTVDataAttribute  
 {3109CFE8-DCA4-4272-BD4E-605AF9D675A1} IRService.IRServiceManager  
 {31C88FF0-2111-44BD-A121-61DE9CD0412D} CBVA DMO wrapper filter  
 {33D8C85A-B8C1-4828-B51A-4F3349AD5F9E} RecordingEventsMediator Class  
 {3429E395-176B-4a0a-863D-FCA6B19073BA} GeneralProperties Class  
 {3630AB4B-C0D2-4C1B-B7E7-73A2CF9A4521} Mcx2Install Class  
 {3697C5FA-60DD-4B56-92D4-74A569205C16} Tablet PC Correction for Windows Journal  
 {37BEC31C-370A-4324-8933-50E30B1C9901} PSFactoryBuffer  
 {39A4740D-2C8E-4186-A2DF-E3F5DD6025C2} GLIDPlugInISDBSatellite Class  
 {39C42C60-85F5-40ED-BF39-975A0AA0B2A4} HandWritingSkin Class  
 {3B0FB8F1-8882-4C9D-9E35-6C23FB9D8110} BDA Proxy UPnP 1.0 Event-base Streaming  
 Plugin  
 {3B191048-B0AD-4CFE-902C-F51140AA77ED} AudioCD Class  
 {3B68879A-2CE5-419D-BB70-F39E1F66B06F} MathRecognizer Class  
 {408A179C-A68C-4c49-ACD3-65BA221E6A71} KeystrokeGenerator Class  
 {40B6664F-4972-11D1-A7CA-0000F87571E3} Scripts (Startup/Shutdown)  
 {40B66650-4972-11D1-A7CA-0000F87571E3} Scripts (Logon/Logoff)  
 {40B66660-4972-11D1-A7CA-0000F87571E3} Scripts (Startup/Shutdown)  
 {40B66661-4972-11D1-A7CA-0000F87571E3} Scripts (Logon/Logoff)  
 {41DADF7D-609C-11DB-B5B9-000CF179CDD7} Microsoft.MediaCenter.Tags.TagManager  
 {46445657-1F22-11DA-A2D9-00065B83EE53} PSFactoryBuffer  
 {478DD7E7-228D-44B7-9854-DFB0E818D8A7} CHTInputModule Class  
 {48C6BE7C-3871-43cc-B46F-1449A1BB2FF3} Offline Files Cache Control  
 {48E1B01B-5619-4898-8714-DD1897BA07B2} DataBurner Class  
 {494C063B-1024-4DD1-89D3-713784E82044} CoBrmEngine Class  
 {4a8dbdfc-6c55-4c0d-9cb8-65bb711e4a4e} EHomeMCLDropTarget Class  
 {4B635ECB-0887-4015-8CA6-D621362F98D1} ResourceMgr Class

## SOFTWARE OUTPUT

```

{4b7601c1-d292-4902-89f4-583a5ce0c535} EHomePhotosHandler Class
{4CE576FA-83DC-4f88-951C-9D0782B4E376} UIHostNoLaunch Class
{4DF7BC39-C84D-4c80-8950-EDC1D77C9D4B} McxRemoteDvdPlayer Class
{4EA9D6EF-694B-4218-8816-CCDA8DA74BBA} SensorDataReport Class
{4f61ec50-acef-4ae7-b4c6-b19bddc0f745} EHomeVideosHandler Class
{4F637904-2CAB-4F0E-8688-D3717EBD2975} Group Policy About Information
{4F71C8B1-F8DE-4773-A6CB-E507C2D5819C} IRService.CSetTopBox
{4fabef66-4cf2-4222-a7c4-0acd3fe75b17} MCMDE NETCHANNEL ACTIVATE
{4FDDEA74-513D-4454-90B4-4AB1011157AD} Stationery Class
{509443A8-B499-4d72-9222-52B82980D8AB} TVThumbnailCache Class
{50A7B286-7D23-41E6-9440-4DAEE00DC5F0} LogicalSensorManager Class
{50D9196A-DD32-4f64-9BD1-20AB9175858E} InstallEventsMediator Class
{565E978D-AC10-443A-A2C8-165C2DA1B5FC} Sticky Notes Windows Desktop Search
Protocol Handler
{56C4F5A2-E217-4610-83CC-89F09E07782B} NbCompositeLayer Class
{56ff6ee0-0f4e-4bb1-bf37-ed8a49c455ae} McxRemoteFilePlayer Class
{5971EC44-072A-41b7-8E67-D9E045CC196D} AppIdMmcPolicyHandler Class
{599141B3-B243-11DB-8460-00123F76E1F7} iTvHost Class
{599141D2-B243-11DB-8460-00123F76E1F7} Microsoft.MediaCenter.iTv.AudioClipFactory
{599141D4-B243-11DB-8460-00123F76E1F7}
Microsoft.MediaCenter.iTv.BackgroundImageFactory
{59B7D16A-C309-47C4-9667-363B9B8D8255} PSFactoryBuffer
{5A09F97B-708A-404D-871F-1D414F6F83B4} GLIDLoaderDispatcher Class
{5BBACA3E-9775-46F8-8301-48817E09D92A} MhegAddIn Class
{5cc76543-0f98-47a8-afa2-208562ef9454} MCESetTopBox Class
{5d8539fa-9e3b-459f-8118-020b5ef1796e} JNT Persistent Handler
{5ea4f148-308c-46d7-98a9-49041b1dd468} Mobility Center Control Panel
{5ED98377-87A3-4d86-81F7-3E46E0342833} AdvancedProperties Class
{6101F767-998E-452B-B54A-E836DD486BAD} SensorClassExtension Class
{62ADD3C3-2648-41E3-A142-5F379BE9229A} IP Receiver Data Plugin
{63E23168-BFF7-4E87-A246-EF024425E4EC} RSOP Context Menu
{64445657-9101-11d9-994B-00301BB132BA} InkItem Class
{6570B2AA-1F63-4959-9D98-C12ABB483DFC} BurnDevice Class
{65bbb826-08fd-48da-922f-99dbd23a8590} MCMDE MPEG2 SINK ACTIVATE
{66588FF3-290B-41b9-99CA-A90A86C73499} DefinitionParser Class
{673F14E0-1875-42a1-90F9-647F4AD9DB92}
{6B19643A-0CD7-4563-B710-BDC191FCAD3B} TSFstateManager Class
{6B7C8A70-35FC-478A-B652-ADD50536E270} PSFactoryBuffer
{6CE51F75-0448-438e-B9CA-69C352A248A7} Sensors CPL Change Device Permission LUA
Helper
{6DC3804B-7212-458D-ADB0-9A07E2AE1FA2} Resultant Set of Policy
{6e2822ca-f234-45da-8c4c-1408e18981d1} EHomeDVRDropTarget Class
{6FDEDD65-AC51-43CA-B2D0-9EB5D1155D03} MediaCenterSSO Class
{70445657-5AB0-11d9-A4E5-00301BB132BA} InkStore Class
{73EB8142-4A74-49FD-A0FC-05FAEED4CD51} Advanced Audit Policy Group Policy Editor
Extension
{74ABD359-DD57-46b2-B459-B8FC803E67D4} TipSettings Class
{76AE5F57-B7C9-421f-B55E-FB25144317B6} Sensors CPL Change Description LUA Helper

```

## SOFTWARE OUTPUT

```

{76DC8129-0A40-45eb-B0DC-09E8C6CDE9D} NbTextLayoutPageProp Class
{76EFD608-E0CE-4887-98E2-F931363C4BC5} SideShowClassExtension Class
{76FD18F9-45AC-456d-8449-E1DA59B5E3D2} Wtv2dvrmS Class
{77A1C827-FC D2-4689-8915-9D613CC5FA3E} SensorManager Class
{77FAEBF1-5708-4413-8CF1-2F92F75EE71D} PSFactoryBuffer
{78F0BBC7-A4EE-4c39-B27B-7BB3955745F8} PBDA Proxy Persistence Manager
{79C43ADB-A429-469F-AA39-2F2B74B75937} SensorCollection Class
{7b6f5efb-45f0-4672-ab4d-4463c5957854} McxMediaController Class
{7E45546F-6D52-4D10-B702-9C2E67232E62} Software installation
{7F6316B4-4D69-4765-B0A3-B2598F2FA80A} RecordingDispatcher Class
{7FA3A1C3-3C87-40de-AC16-B6E2815A4CC8} RecoveryTaskWrapper Class
{802B1FB9-056B-4720-B0CC-80D23B71171E} Microsoft PenInputPanel Control
{807C1E6C-1D00-453f-B920-B61BB7CDD997} Microsoft TipAutoCompleteClient Control
{8278d39b-969e-464e-9f87-fba297879ce3} McxAsyncRemotePlayer Class
{83FEFA40-6F67-4244-AA04-1E590C1CB1D9} TextContributor Class
{84DE202D-5D95-4764-9014-A46F994CE856} Administrative Templates - Starter GPO
(Computer)
{84DE202E-5D95-4764-9014-A46F994CE856} Administrative Templates - Starter GPO
(User)
{8613E14C-D0C0-4161-AC0F-1DD2563286BC} Correction Widget Class
{8752858E-C146-4a7b-9CE8-A978DCAD03C6} DefinitionLoader Class
{87DBE38C-A22E-43D3-8128-27FFA848A113} IRService.IRUser
{88EBC1EE-F90A-484A-B9C5-8F9C0F37A828} iTV Data Sink
{88EEBD3A-9091-44b8-92A7-F0D595422D90} GesturesProperties Class
{8A51DC27-5A35-4E02-95A3-428BC6244A3C} iTV Data Capture filter
{8A539A30-0653-4E54-91B8-C8CF5DE862A1} RichInkSegment Class
{8BA2F157-CC2D-4d7a-BE0B-99C53DB78F10} NbDocCstg Class
{8BD9A7C7-6370-4A3C-A13F-6EA023A1E75C} Microsoft Network Tuner Manager
{8C24BE77-7E9E-4d5c-85F7-EFC393B5FEC4} NbBaseEditableDocument Class
{8c74d361-c6d8-4e14-b9bf-5412b1530f8d} MCAsyncFilePlayer Class
{8DAC2D4D-A139-468e-94F4-522362EBD7D2} MCAsyncDVDPlayer Class
{8e482066-3e12-4188-86b6-fbc909c7e0d5} AnalogRecorder Class
{8F84CF05-3F6B-43FF-8851-0EC42B4F3849} PSFactoryBuffer
{8F9B42DD-9491-451a-8CCE-812DB368210C} MCSyncDVDPlayer Class
{8FC0B734-A0E1-11D1-A7D3-0000F87571E3} Local Group Policy Editor
{901AB1E6-3EC9-4aae-AEE5-188013A5CC21} RioEventSender Class
{91081579-EE4D-4991-9451-E1725A9DF347}
Microsoft.MediaCenter.Pvr.Service.PvrService
{917D1F24-F668-4B1F-A8E6-7C426ADD48EC} PSFactoryBuffer
{942A8E4F-A261-11D1-A760-00C04FB9603F} Software installation
{95142bf8-5f09-452b-b384-44af84a500c6} MCEIRUser Class
{9859049F-C6D1-4e66-B0F8-188FF1064E3C} CompositeInputItem Class
{98D99750-0B8A-4c59-9151-589053683D73} Windows Search Service Media Center
Namespace Extension Handler
{9968FA8D-401B-41c1-8987-362AABA71C2D} WMDRM Plugin
{9A630456-078D-43d3-9F1D-DF7A5BC0FA44} Default Location CPL Data Handler LUA
Helper
{9b359d1b-ad5c-412f-a654-a431424359de} Offline Files Profile Notify Handler

```

## SOFTWARE OUTPUT

```

{9C4D3346-650D-472d-A867-6F595B39D973} AuditPolicyGPHandler Class
{9CE24FD4-94CB-4a9a-A19D-1B0F819005B7}
{9e3b7257-da6e-419c-9601-fcf13774a9aa} MCMDE LPCM SINK ACTIVATE
{9F074EE2-E6E9-4d8a-A047-EB5B5C3C55DA} HwTextInsertion Class
{9F22CFEA-CE07-41ab-8BA0-C7364AF90AF9} Microsoft TV Subtitles Decoder
{A1E6E578-A831-4803-8DC3-433843B1E19C} GLIDLoaderWrapper Class
{A24BCC4A-448D-41CA-92BB-3DC15D81C16C} MediaStatusSession Class
{A48E70A4-8E15-4465-9D85-CCE9E63F8AAB} EHomeVideoDropTarget Class
{A4E118DF-B9E5-4B42-888C-065CEAF8DDC3} Mcx2Uninstall Class
{A5CF917A-0F75-4b29-A0A0-5348E501DA59} RecoveryTaskMonitor Class
{A666634D-333F-4CC9-AF78-65ED7DB1D6C3} PSFactoryBuffer
{A68B20E5-0E4B-4E79-8310-FEF1912C9C66} IP Sender Data Plugin
{a81d181b-0fd4-4442-91a1-b6febfa1dc6} Journal File Filter Class
{a8298e0c-7201-470e-84d5-728cff85bcbf} MCEMediaOutputDevice Class
{A96434FF-30F1-430E-B568-DCCCB831FFCE} JPNInputModule Class
{A989DC2B-5E13-4426-9BD4-F666D96F15F8} WMDRM Plugin
{AFD8EA5A-2B6E-4504-B681-C6E8BAD64BB6} EhEPGdatEventsMediator Class
{AFE0D06B-E242-47ea-A987-74EB2D1030E6} NbTextLayoutPage Class
{AFF4A44B-1897-453F-B6A1-BE152D0A0F75} DvbSiParser Class
{B1C3DB01-7D82-4BA2-AA5D-4F1371302241} PSFactoryBuffer
{B29D466A-857D-35BA-8712-A758861BFEA1}
Microsoft.GroupPolicy.AdmTplEditor.GPMAdmTplEditorManager
{B6B44A97-B802-4d6e-9846-3AB9C0965C43}
{B6F9C8AE-EF3A-41C8-A911-37370C331DD4} Administrative Templates (Computers)
{B6F9C8AF-EF3A-41C8-A911-37370C331DD4} Administrative Templates (Users)
{B7A44F26-0114-4285-B4BA-C9E78C4F9416} NbDocView Class
{B8CD2E5E-AACF-4F92-9F3B-2E753B9410EE} GLIDPlugInISDBTerrestrial Class
{BA5BD097-67CF-48f0-8661-38A49BF4903F} ehGLIDNetOPlugIn Class
{BA9FCBAC-3AE4-46BF-B7BA-669498CCC8DE} CPreferredTIPState Class
{BACF5C8A-A3C7-11D1-A760-00C04FB9603F} Software installation
{BF0B4450-B1F8-4238-98B1-9CE4544D5673}
{c1ea08ae-1451-4b43-a19b-12298656ad35} DigitalRecorder Class
{C24B9728-35A2-4C36-B763-2B007CFAF70F} CMFNetworkCongestionControl Class
{C3A61ACF-9BE4-4e35-9A76-810AF62191E6} MCASyncVcdPlayer Class
{C4457F51-993A-4b98-A19B-EC2B4F0DA087} AppLocker Configuration Tool
{C4D6E899-E38A-4838-9188-0B98EE3175E6} ProgrammabilityManager Class
{C4D77430-755D-4E19-A6E1-AA8CA5E0E7BC} TipTsFData Class
{C561816C-14D8-4090-830C-98D994B21C7B} MathInputControl Class
{C77A3910-BAB0-4A38-A0A1-405FA9257C1B} English3x4InputModule Class
{C78A4622-A033-4dab-94E8-43DE54B461F4} RecoveryTasks Class
{CA4DEAB8-2C34-42B7-B4A5-78CD28A2D54F} PSFactoryBuffer
{CB445657-116F-11D8-941D-00065B83EE53} PSFactoryBuffer
{CD621DE4-2AA5-4468-ADF1-087A05891DA7} EhEPGdatWrapper Class
{D02B1F72-3407-48ae-BA88-E8213C6761F1} Administrative Templates (Computers)
{D02B1F73-3407-48ae-BA88-E8213C6761F1} Administrative Templates (Users)
{D09D1E04-D590-39A3-B517-B734A49A9277} PSFactoryBuffer
{D10DF471-8E15-4524-A8B6-00779A1231FD} GLIDPlugInDVBTerrestrial Class
{D145BF00-4389-49E9-B3A0-4178719550CD} NetBridge

```

## SOFTWARE OUTPUT

```

{D44CBB4F-743E-4818-8077-C47F666CA7EE} BackgroundScanner Class
{D5C82393-AB49-47e9-BE80-B7801443BE43}
{D6E88812-F325-4dc1-BBC7-23076618E58D} TsfManager Class
{D88B44DB-6C5C-4501-B7FC-3E7476275C84} AtscPsipParser Class
{D9B59177-33A7-4D76-9D51-2A996699EB25} MCVideoPresenter Class
{DA77D991-4499-4f01-81D4-5127E93495BE} IP Receiver Data Plugin
{DC79858F-F8D2-47F7-9A1E-C879CB59A4F9} Digital Keystone BDA Proxy Persistence
Manager
{DD8D8457-6DE1-40d3-83B2-53AAC340715C} KeyStrokeMonitor Class
{DE13E041-1416-430e-9C2F-F7A548D26B3B} ScanConfigWrapper Class
{E05FDDDED-C4A7-4338-80D7-7577655D5412} VideoAudioBurner Class
{E25E57E9-DA9C-4A35-A0D8-CFB5EA6AF7E6} Advanced Audit Policy Configuration
{E4E54B1D-1AC1-405c-B62A-E11CD87F2261}
{E55A0B49-2F73-44D4-AD66-48966DED31BA} Media Center Extender Encryption Filter
{E62456F4-62AC-45CB-99DE-4E0F6B6062D7} SBEDeviceManager Class
{E7F34D0A-582E-4a48-98BA-6E58AAA3AD4C} Sensors PropertyPage Host
{E8DF2799-8F1B-4b60-B30F-AED6BBF39625} EhepgdatDispatcher Class
{E94137E0-92ED-4579-9251-18AF2A08CCD1} Tablet Tip Soft Keyboard Skin Class
{E97CED00-523A-4133-BF6F-D3A2DAE7F6BA} Sensor Class
{E98DBAEF-45AD-4de1-84E7-3FCFA79FF1FA} PBDASiParser Class
{E9950154-C418-419e-A90A-20C5287AE24B} Sensors
{EA23DFB6-E23F-4b94-B1A4-095D6E84493C} EnumRecorderGraph Class
{EACFAA1F-A6CB-4d4a-83D9-810F84C11803}
{EBDD6BF3-AF35-4bf1-9EE3-335A3F5DE0FF} NbAccessibleObject Class
{ED233797-F47D-475e-9FCA-3D549E4DDAA4} EhTraceProvider Class
{ED834ED6-4B5A-4bfe-8F11-A626DCB6A921} Personalization Control Panel
{ED87EFF3-FF22-404E-B2BD-BC3841BDCB2C} EHomeMusicDropTarget Class
{EFB23A09-A867-4BE8-83A6-86969A7D0856} PSFactoryBuffer
{F0B14D86-2673-443b-AE9B-1E274E229D19} GLIDPlugInPAL Class
{F1ED7D4C-F863-4de6-A1CA-7253EFDEE1F3} AppIdPolicyHandler Class
{F25E9F57-2FC8-4EB3-A41A-CCE5F08541E6} CPenIMX Class
{f2ce09f6-d836-4029-be4c-5793ba9f14ec} McProxy Class
{F3B4F2E9-CCCC-49aa-B0B2-2C4A02E69A37} TabTipUI Class
{F3EFA86C-6B4F-434d-A6FF-BA797494C9B2} StateController Class
{F3F5824C-AD58-4728-AF59-A1EBE3392799} Sticky Notes Namespace Extension for
Windows Desktop Search
{F4396DC6-E851-4D3A-8D01-34E6949F3500} RecorderMgr Class
{f4a5145b-260d-437f-89c4-66d81c22e9b6} OutputProfileMgr Class
{F54879F6-3424-4d7a-999F-9095ABCD3FC} UPnP 1.0 Property Plugin
{F87CB264-80B7-4df8-9E62-ABC259074CF6} NbRioEventSink Class
{F88A4455-BEB8-4D91-8C13-6807B0147727} CHHInputModule Class
{F9B189D7-228B-4F2B-8650-B97F59E02C8C} Microsoft TextInputPanel Object
{FAC07F06-B005-49df-A25A-BD5D091FCC81} GLIDPlugInDVBSatellite Class
{FC138128-D766-4f2a-9EA6-6C88E3EC2301} NbBitmapLayer Class
{FC8E372E-8847-4E45-B724-F676B1CACC7D} UPnP 1.0 Property Plugin
{FD76C304-255F-4446-A895-6E1967EC4FDC} AppLocker Group Policy Editor Extension
{FD8D7237-49E4-4B99-A580-ACA91ED6FCDA} RioTabletInput Class

```

Tue Apr 12 08:28:58 2011 Z

## SOFTWARE OUTPUT

{07C0A9A9-6308-4C15-B818-225D4F3FBF48} Microsoft.MediaCenter.GlidHost.GLIDLoader  
 {09F81337-D568-41d1-A177-D6779AF55847} WBEM WIN32\_TSVIRTUALIPSETTING Provider  
 {10CFC467-4392-11d2-8DB4-00C04FA31A66} Offline Files Folder Options  
 {1A056BDB-8B45-462f-8D85-CAC6BDCD2A31} Microsoft.MediaCenter.GlidHost.ScanConfig  
 {1FF28512-6C1F-4CC2-BB1D-948DD60DB711}  
 {28F4700C-44EB-4BD8-BC25-95812DE98E08} PPCNode Class  
 {2F248FAD-47C5-42a8-9672-61095D712258}  
 {357b663c-d9fa-4188-99af-2943920f96c5} PSFactoryBuffer  
 {39524FB7-028F-4035-8C2B-8E65D2B17E67} WBEM WIN32\_TSSSESSIONDIRECTORY Provider  
 {3F13AB10-AE95-48AA-8C94-533730760A20} PMCRotNode Class  
 {42D69529-136E-49D6-8407-3026853038BF} PMCComponent Class  
 {450D8FBA-AD25-11D0-98A8-0800361B1103}  
 {45F26E9E-6199-477F-85DA-AF1EDFE067B1} SessionAgent Class  
 {474C98EE-CF3D-41f5-80E3-4AAB0AB04301}  
 {4B0A2997-E555-4F84-B45B-68AB8BC57635} RdpEndpoint Class  
 {4C8A0917-F587-4ECF-9C89-48147528F4E1} WBEM WIN32\_TSGENERALSETTING Provider  
 {4E77131D-3629-431c-9818-C5679DC83E81}  
 {4FE8C25F-C8E9-4322-98EE-A11E117CF049} MachineComponentData Class  
 {50422459-63B3-4e9f-93C7-7B068517C027}  
 {599141D5-B243-11DB-8460-00123F76E1F7}  
 Microsoft.MediaCenter.iTv.CiTvCaptionControl  
 {599141D6-B243-11DB-8460-00123F76E1F7}  
 Microsoft.MediaCenter.iTv.CiTvOverlaySurface  
 {599141D7-B243-11DB-8460-00123F76E1F7} Microsoft.MediaCenter.iTv.CiTvServiceInfo  
 {599141D8-B243-11DB-8460-00123F76E1F7} Microsoft.MediaCenter.iTv.CiTvSession  
 {599141D9-B243-11DB-8460-00123F76E1F7} Microsoft.MediaCenter.iTv.CiTvStreamEvents  
 {599141DA-B243-11DB-8460-00123F76E1F7} Microsoft.MediaCenter.iTv.CiTvStreamInfo  
 {599141DB-B243-11DB-8460-00123F76E1F7}  
 Microsoft.MediaCenter.iTv.CiTvStreamSelector  
 {599141DC-B243-11DB-8460-00123F76E1F7} Microsoft.MediaCenter.iTv.CiTvTuning  
 {599141DD-B243-11DB-8460-00123F76E1F7} Microsoft.MediaCenter.iTv.CiTvVideoSurface  
 {599141DE-B243-11DB-8460-00123F76E1F7}  
 Microsoft.MediaCenter.iTv.CiTvMediaCenterSettings  
 {647BD8C2-658B-4ECA-ABC7-FC5C0BF1704D} WBEM WIN32\_TSCLIENTSETTING Provider  
 {68E1DF8C-9512-4801-A105-25A44DCCB164}  
 {69486DD6-C19F-42e8-B508-A53F9F8E67B8} Offline Files Service Control  
 {69D76D1B-B12E-4913-8F48-671B90195A2B} Microsoft WBEM WMI Policy Status Provider  
 {6B56A227-7150-4A1F-A114-C959EB8F8C24} Software Installation Group Policy User  
 Profile Notification  
 {6BD6AECA-AFB0-45B7-BAC4-F292EC0F3F41} WBEM Win32\_TERMINALSERVICESSETTING Provider  
 {71B804C5-5577-471D-8FE5-C4A45B654EB8} Windows SideShow AutoWake Configuration  
 Helper  
 {7295965A-230A-4F34-AD5F-B15C9120F6E4}  
 {74628299-57EC-4F12-BA1C-08B477BF447A} WBEM WIN32\_TERMINAL Provider  
 {750fdf10-2a26-11d1-a3ea-080036587f03} Offline Files Synchronization Handler  
 {76052C5C-2EB4-4C40-B1F1-2A5C8554590A} Connect to a Network Projector  
 {7757BA9B-7986-4866-B53F-A31E89FCBA15} WBEM WIN32\_TSNETWORKADAPTERLISTSETTING  
 Provider



## SOFTWARE OUTPUT

```

{7970614A-BD82-439E-A828-CC96F8E91428} WBEM WIN32_TERMINALSERVICE Provider
{7C606A3F-8AA8-4E36-92D6-2B6AFEC0B732} PMCPrintQueueViewExtension Class
{7CCA6768-8373-4d28-8876-83E8B4E3A969} SDPWmiJob Class
{7EFA68C6-086B-43e1-A2D2-55A113531240}
{86950435-ED12-42ef-A807-061E5E7CA99F}
{9209B7D1-6DA5-43E4-BCD1-F2BE497635E7} RdpEndpoint Class
{9A17DFD1-34FA-4D61-B9BB-3A1097E7FADF} WBEM WIN32_TSENVIRONMENTSETTING Provider
{A0ADD4EC-5BD3-4f70-A47B-07797A45C635}
{AAEAE72F-0328-4763-8ECB-23422EDE2DB5} Microsoft WBEM WMI Policy SOM Provider
{AFDB1F70-2A4C-11d2-9039-00C04F8EEB3E} Offline Files Folder
{B03B16C7-35A7-4A55-BEF1-8876E1CE2F45} PMCAbout Class
{B490264C-8D8F-40FD-B1BE-CD69AD779EC1} WBEM WIN32_TERMINALSERVICETOSETTING
Provider
{BA4EAC04-AFCE-441A-A4F0-C4A97545425A} WBEM WIN32_TERMINALTERMINALSETTING
Provider
{BB5331F1-D8FF-4DDB-8A8F-2DF901123B33} PPCRootNode Class
{BDE24877-01D7-4103-9704-F0EC82FA7CE9} UserComponent Class
{BDF9E8B8-6C66-4E45-BA15-E050393DD079} WBEM WIN32_TSACCOUNT Provider
{BE9B3133-250B-44A5-A278-C532B7B7FF76} WBEM WIN32_TSSSESSIONSETTING Provider
{C41FF872-07B1-4926-819B-8C94E6B1FBB9} WBEM WIN32_TSLOGONSETTING Provider
{C51F0A6B-2A63-4cf4-8938-24404EAEF422}
{CB35832D-0C2C-41A9-84E1-A7CD1E0C6254} UserComponentData Class
{CCBA37FC-982B-433B-8AC2-455E616A8559} WBEM WIN32_TSSSESSIONDIRECTORYSETTING
Provider
{D06342BD-9057-4673-B43A-0E9BBBE99F11} PMCComponentData Class
{D25E0260-AAB7-48CB-A192-4D73D2FD375F} WBEM WIN32_TSNETWORKADAPTERSETTING
Provider
{D3667F1E-CCB8-4A69-99DF-59A2B2A6753F} Windows SideShow Device Configuration
Helper
{DA2B8720-3354-4FAB-B838-B1472667C8E9} Microsoft.MediaCenter.GlidHost.GLIDHost
{DB285FF6-02D5-4D5D-BC48-A793BF9A90F2}
Microsoft.MediaCenter.SideBarGadget.MCESideBarCtrl
{DB49BBEB-C744-49F8-81AC-AF97669D4CB0} PrinterStatusHTMLViewExtension Class
{DBD71B6B-F717-4A61-A914-2337BC50B0D6} WBEM WIN32_TSREMOTECONTROLSETTING Provider
{E51DFD48-AA36-4B45-BB52-E831F02E8316} AutoWakeTaskHandler Class
{E95A4861-D57A-4be1-AD0F-35267E261739} Windows SideShow
{EC278F3A-BFE8-42d5-99C0-E25F5EF4A3D1} WBEM WIN32_TSVIRTUALIP Provider
{EF6EF542-EB19-4986-89D3-143960609251} MachineComponent Class
{F056D291-A2AB-45f7-8EE4-40454493B351} Windows SideShow PropertyPage Host
{FA06375D-F0A4-4A47-AD8D-148595F1E0B8} WBEM WIN32_TSPERMISSIONSSETTING Provider
{FA3F3DD9-4C1A-456B-A8FA-C76EF3ED83B8} Offline Files Background Synchronization
Task Handler
{FD3659E9-A920-4123-AD64-7FC76C7AACDF} Offline Files Setting Object
{FF87090D-4A9A-4f47-879B-29A80C355D61} GadgetsManager Class
Tue Apr 12 08:28:44 2011 Z
{BFC006EE-B806-4C2A-A938-6D3344781512}
Sun Nov 21 03:40:13 2010 Z
{0F0C09C5-601E-4396-BCD0-CDB343D7F657} SSTP Configuration Configuration Notify

```

## SOFTWARE OUTPUT

## Object

{6E65CBC0-926D-11D0-8E27-00C04FC99DCF} Dial-Up Client Configuration Notify Object  
 {6E65CBC1-926D-11D0-8E27-00C04FC99DCF} Dial-Up Server Configuration Notify Object  
 {6E65CBC3-926D-11D0-8E27-00C04FC99DCF} NdisWan Configuration Notify Object  
 {6E65CBC4-926D-11D0-8E27-00C04FC99DCF} PPTP Configuration Configuration Notify

## Object

{6E65CBC5-926D-11D0-8E27-00C04FC99DCF} Steelhead Router Configuration Notify

## Object

{6E65CBC6-926D-11D0-8E27-00C04FC99DCF} L2TP Configuration Configuration Notify

## Object

{7177c4bd-e20a-4140-ad8a-998e7a2d18c0} AGILEVPN Configuration Configuration

## Notify Object

{e949da38-c39d-4460-8ea7-a39152c56836} PPPOE Configuration Configuration Notify

## Object

Sun Nov 21 03:39:53 2010 Z

{0C41D1E6-9D16-41ED-9CDD-D0665039857B} Microsoft TCP/IP Version 6 Configuration

## Notify Object

{A907657F-6FDF-11D0-8EFB-00C04FD912B2} Microsoft TCP/IP Configuration Notify

## Object

Sun Nov 21 03:39:29 2010 Z

{CD000001-8B95-11D1-82DB-00C04FB1625D} CDOMessage Class  
 {CD000002-8B95-11D1-82DB-00C04FB1625D} CDOConfiguration Class  
 {CD000004-8B95-11D1-82DB-00C04FB1625D} CDO DropDirectory class  
 {CD000005-8B95-11D1-82DB-00C04FB1625D} SMTP OnArrival Script Host Sink Class  
 {CD000006-8B95-11D1-82DB-00C04FB1625D} NNTP OnPost Script Host Sink Class  
 {CD000007-8B95-11D1-82DB-00C04FB1625D} NNTP OnPostFinal Script Host Sink Class  
 {CD000008-8B95-11D1-82DB-00C04FB1625D} SMTPConnector Class  
 {CD000009-8B95-11D1-82DB-00C04FB1625D} NNTPPostConnector Class  
 {CD000010-8B95-11D1-82DB-00C04FB1625D} NNTPFinalConnector Class  
 {CD000011-8B95-11D1-82DB-00C04FB1625D} NNTPEarlyConnector Class  
 {CD000012-8B95-11D1-82DB-00C04FB1625D} NNTP OnPostEarly Script Host Sink Class  
 {E3A9BD50-51AE-410f-9706-0BA0D68B9A94} Scavenged Files Cleanup

Tue Jul 14 04:54:39 2009 Z

{0F7434B6-59B6-4250-999E-D168D6AE4293}  
 {1D6322AD-AA85-4EF5-A828-86D71067D145} UIAnimationTransitionLibrary  
 {2854F705-3548-414C-A113-93E27C808C85} Enhanced Storage Context Menu Handler

## Class

{32665929-D77E-4ab5-8C08-FBF409B8A233}  
 {32BA16FD-77D9-4AFB-9C9F-703E92AD4BFF} CtTuner Class  
 {36F54939-CD3B-4C73-92D5-F9A389ED631C} Enhanced Storage Autoplay Handler Class  
 {4C1FC63A-695C-47E8-A339-1A194BE3D0B8} UIAnimationManager  
 {641ABA69-56FD-4029-A445-4D8375D3A699} UIAnimationDiagnostic  
 {886D29DD-B506-466B-9FBF-B44FF383FB3F} EnhancedStorageSiloAction Class  
 {8A9B1CDD-FCD7-419c-8B44-42FD17DB1887} UIAnimationTransitionFactory  
 {9113A02D-00A3-46B9-BC5F-9C04DADDD5D7} Enhanced Storage Data Source  
 {926749fa-2615-4987-8845-c33e65f2b957}  
 {af076a15-2ece-4ad4-bb21-29f040e176d8} EnhancedStorageACT Class  
 {BFCDA40C-06B6-4384-B768-0DAA792C380E} UIAnimationTimer

## SOFTWARE OUTPUT

```

{C608E099-892D-4628-B6A2-97257B014E2E}
{cb25220c-76c7-4fee-842b-f3383cd022bc} EnhancedStorageSilo Class
{CC55EE92-FE67-43C9-95E7-E646918A4A04} Enhanced Storage Command Handler
{D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D} Enhanced Storage Icon Overlay Handler
Class
{f4d8c39a-f43d-42b4-9bdf-4e48d3044ba0} Name Resolution Policy
{fe841493-835c-4fa3-b6cc-b4b2d4719848} EnumEnhancedStorageACT Class
Tue Jul 14 04:54:38 2009 Z
{D212B88E-8365-4CA9-BC4E-CFA4251F6B5F} NdisCap Notify Object
{FCDC2CF5-ABCD-4BA5-94DA-1823AE06FE2B} CorrelationEngine Class
Tue Jul 14 04:54:37 2009 Z
{D17D1D6D-CC3F-4815-8FE3-607E7D5D10B3} Text to Speech Control Panel
Tue Jul 14 04:54:36 2009 Z
{ca767aa8-9157-4604-b64b-40747123d5f2} RegistryIdleBackupHandler
Tue Jul 14 04:54:32 2009 Z
{0003000A-0000-0000-C000-000000000046} Bitmap Image
{08229782-89C8-4028-BB74-75BB58EF1488} IP Security Monitor
{1fda955b-61ff-11da-978c-0008744faab7} Detection And Sharing
{1fda955c-61ff-11da-978c-0008744faab7} PSFactoryBuffer
{57C596D0-9370-40C0-BA0D-AB491B63255D} IP Security Monitor
{A17DA8D0-F67D-47A0-9EC4-19C486383206} IP Security Monitor
{A2A54893-AAF2-49A3-B3F5-CC43CEBCC27C} Network Access Protection GPEdit Extension
{ABB78EBD-45BD-415B-9466-5C2A0F25CACE}
{B3408A2F-8DDA-1197-FBD5-2CE69A2DEFC0} @%systemroot%\system32\eqossnap.dll,-30001
{B3408A2F-8DDA-1197-FBD5-2CE69A2DEFC1} @%systemroot%\system32\eqossnap.dll,-30001
{C1060E7E-7939-44A5-99C3-A6DCCD92AED0} PSFactoryBuffer
{D3E34B21-9D75-101A-8C3D-00AA001A1652} Paintbrush Picture
{DEA8AFA0-CC85-11D0-9CE2-0080C7221EBD} Create and edit Internet Protocol Security
policies
{DEA8AFA1-CC85-11D0-9CE2-0080C7221EBD} Create and edit Internet Protocol Security
policies
{DEA8AFA2-CC85-11D0-9CE2-0080C7221EBD} Create and edit Internet Protocol Security
policies
{ff258fc0-99b1-4297-b857-539ad9bc13ed} Cert Enrollment Class
Tue Jul 14 04:54:31 2009 Z
{06993B16-A5C7-47EB-B61C-B1CB7EE600AC} Create and edit Wired policies
{22BDC741-73F0-41DB-9463-E343DEF3E376} PSFactoryBuffer
{24FF4FDC-1D9F-4195-8C79-0DA39248FF48} Quarantine Private SHA Binding class
{2D4156A2-897A-11DB-BA21-001185AD2B89} Network List Manager Snapin
{2D4156A5-897A-11DB-BA21-001185AD2B89} Network List Manager Snapin About
Interface
{388D606F-AF7B-4AD2-AC22-6B4FE70CE286} Create and edit Wired policies
{38B22A43-49A8-45ab-BEB7-9137A488B1D3} Quarantine Private QA Management class
{44C39C96-0167-478F-B68D-783294A2545D} Manage Network Names
{677126ed-2a91-40ff-8c52-06181c064573} NAP Elevated class
{8E594310-16CA-4a00-932F-F70969F990C0} Quarantine System Health Agent Binding
class
{9443B89B-6564-496a-B19C-6C6D22709045} Quarantine Enforcement Client Binding

```

## SOFTWARE OUTPUT

class

```
{9a010fcc-488b-4836-94fd-c489f8e1ed7d} NDIS Helper Class
{A1E7036D-72A1-4529-B108-0C3C9E92D424} Create and edit Wired policies
{B475F925-E3F7-414C-8C72-1CEE64B9D8F6} PSFactoryBuffer
{bc65fb43-1958-4349-971a-210290480130} Ncd Property Page
{C330DE32-29C7-4cf2-9807-74BCB5486A37} Nap Client WMI Provider Class
{D60795C3-F2A5-45b1-A731-2516E7EAB8EB} NAP Helper Class
{d6afe216-3106-4e91-953f-ffa26064c8ee} Nap Config Write Class
{DCBCA92E-7DBE-4eda-8B7B-3AAEA4DD412B} Quarantine Private QEC Binding class
{DD373F1A-7227-4e3c-9AFB-98C288CF1956} Quarantine EnforcementClient Connection
```

class

```
{e5fae3b3-1ac8-4bd3-87e6-48eff509ddaa} Nap Certificate Relying Party class
{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c} Nap Config Read class
{eb082ba1-df8a-46be-82f3-35bf9e9be52f} Quarantine Agent Management class
```

Tue Jul 14 04:54:30 2009 Z

```
{02703d01-d9ab-422c-bbb7-37a0fab7642} WCN NCD Pairing Handler Class
{0273c57c-6693-4444-b20c-a62a3b185b7e} Device Display Objects Proxies
{0BD7E521-4DA6-42D5-81BA-1981B6B94075} PSFactoryBuffer
{0D0D66EB-CF74-4164-B52F-08344672DD46} UPnP Service Provider Class
{145B4335-FE2A-4927-A040-7C35AD3180EF} SSDP Provider Class
{1B0D2365-B3A3-4759-9533-D6861E86DE32} IUninstallProvider_PSFactory
{1E1DAECB-F640-416d-96A3-2BC8AFDF6059} IUninstallElevatedHandler_PSFactory
{2DA6AA7F-8C88-4194-A558-0D36E7FD3E64} Create and edit Wireless policies
{35b1d3bb-2d4e-4a7c-9af0-f2f677af7c30} WNet Provider Class
{383b69fa-5486-49da-91f5-d63c24c8e9d0} Device Pairing Handler Class
{3B2D194D-F107-4489-ABF8-57A125275E4E} Bluewire General Property Sheet
{4876DC0E-F963-4227-9A8F-19872B75D231} Storage Devices Handler
{5C0D19E4-A364-4ef6-9288-DBD194593879} Device Center General Property Sheet
{5F884992-EE6D-418B-9E6C-0C2A0FA94D17} Device Center Hardware Property Sheet
{65E6AC96-4B9B-47EA-AF5C-5DFCC72DCE26} PSFactoryBuffer
{70799824-b3ba-4157-96cb-a34d6170c96f} WindowsInfo.xml parser
{71455ADC-0A77-405F-BF67-EA663D276653} Bluetooth MTP Devices Menu
{7754801c-b01d-4d74-84cb-dfd70669ffbe} DeviceInfo.xml parser
{8101368E-CABB-4426-ACFF-96C4108120CD} Plug and Play Provider Class
{827CE1A1-8255-4165-8C83-8379F8C127AE} Create and edit Wireless policies
{89A502FC-857B-4698-A0B7-027192002F9E} Bluewire Unpairing Handler
{9197e04d-2b9f-4849-8bf7-75294eb5c043} User Mode Bus Driver Class
{A8A91A66-3A7D-4424-8D24-04E180695C7A} Device Center
{B8A27942-ADE7-4085-AA6E-4FADC7ADA1EF} PNPX Pairing Handler Class
{b8fb4ad7-ea4a-4b47-bfdc-bfc94160a8ea} Device Display Object Function Discovery
```

Provider

```
{c282ddad-08b1-494e-951f-d32b89024142} DXP Properties parser
{C2B136E2-D50E-405C-8784-363C582BF43E} DeviceCenter Initialization
{C97FCC79-E628-407D-AE68-A06AD6D8B4D1} AssociatedDevicePresence Class
{cee8ccc9-4f6b-4469-a235-5a22869eef03} PNPX Association Class
{d2e86c4f-ea06-4a89-bf00-b49706db46e6} DDO Resource Info
{D3DCB472-7261-43ce-924B-0704BD730D5F} WS Discovery Provider Class
{D88EC52B-8D57-49e1-9EB3-4D267D68A2AE} Bluewire Elevated Unpairing Handler
```

## SOFTWARE OUTPUT

```

{DD468E14-AF42-4D63-8908-EDAC4A9E67AE} Create and edit Wireless policies
{f59aa553-8309-46ca-9736-1ac3c62d6031} Device Display Status Manager
{F77C0A7D-7395-45c5-BDFC-B096BF6C4DA0} Bluewire Paired Devices Menu
Tue Jul 14 04:54:29 2009 Z
{17B75166-928F-417d-9685-64AA135565C1} Image Transcode
{227ec397-6791-4ac6-a762-2f70f99015c2} IAS Netsh XML Helper
{3F30C968-480A-4C6C-862D-EFC0897BB84B} Photo Extract Image
{48da6741-1bf0-4a44-8325-293086c79077}
{5f6c1ba8-5330-422e-a368-572b244d3f87} PSFactoryBuffer
{6BC09692-0CE6-11D1-BAAE-00C04FC2E20D} IAS Attribute Dictionary
{6BC0969D-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0969F-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096A0-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096C6-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096C8-0CE6-11D1-BAAE-00C04FC2E20D}
{6f13dd2e-ebce-4dd5-a72e-850b2087f5dd} Microsoft Metadata Policy Layer
{83e05bd5-aec1-4e58-ae50-e819c7296f67} PSFactoryBuffer
{8c2031f1-b169-4e7c-9cb0-56f18d7b0c01} IAS XML Data Store
{9d1b93f1-2e5f-4fdb-a95b-dad8d47e28d8} RPC Helper Class
{a38b883c-1682-497e-97b0-0a3a9e801682} IPropertyStore Handler for Images
{BAE86DDD-DC11-421C-B7AB-CC55D1D65C44} PSFactoryBuffer
{BC94D813-4D7F-11d2-A8C9-00AA00A71DCA} SdoService Class
{BED4D415-7971-4310-AA07-6AC15EA06ACC} WinInet Helper Class
{C7657C4A-9F68-40fa-A4DF-96BC08EB3551} Photo Thumbnail Provider
{E9218AE7-9E91-11D1-BF60-0080C7846BC0} SdoMachine Class
{e9970fa4-b6aa-11d9-b032-000d56c25c27} IAS SDO Helper Class
{EAE826D3-ECB5-49ff-BC55-7B318E78C6DD} Dot3BalloonHandler Class
{F1171280-BC35-45d1-8F53-8AB833267899} DNS Helper Class
Tue Jul 14 04:54:28 2009 Z
{01B90D9A-8209-47F7-9C52-E1244BF50CED}
{076C2A6C-F78F-4C46-A723-3583E70876EA}
{0E25DC18-9F5E-48B1-80B3-D124E81B773B}
{1765E14E-1BD4-462E-B6B1-590BF1262AC6}
{22C21F93-7DDB-411C-9B17-C5B7BD064ABC}
{6D68D1DE-D432-4B0F-923A-091183A9BDA7}
{72B624DF-AE11-4948-A65C-351EB0829419}
{7F12E753-FC71-43D7-A51D-92F35977ABB5}
{9CB5172B-D600-46BA-AB77-77BB7E3A00D9}
{A26CEC36-234C-4950-AE16-E34AACE71D0D}
{AA94DCC2-B8B0-4898-B835-000AABD74393}
{AC4CE3CB-E1C1-44CD-8215-5A1665509EC2}
{C17CABB2-D4A3-47D7-A557-339B2EFBD4F1}
{E7E79A30-4F2C-4FAB-8D00-394F2D6BBEBE}
{ED822C8C-D6BE-4301-A631-0E1416BAD28F}
Tue Jul 14 04:54:27 2009 Z
{21D6D48E-A88B-11D0-83DD-00AA003CCABD} TAPI Class
{45234E3E-61CC-4311-A3AB-248082554482} Plug-in Terminal
{4C8D0AF0-7BF0-4f33-9117-981A33DBD4E6} FilePlaybackTerminal Class

```

## SOFTWARE OUTPUT

```

{4DDB6D36-3BC1-11d2-86F2-006008B0E5D2} MSP Class
{7170F2E0-9BE3-11D0-A009-00AA00B605A4} TAPI3 Terminal Manager Class
{72970BEB-81F8-46D4-B220-D743F4E49C95} Volume Shadow Copy WMI Provider
{890CB943-D715-401B-98B1-CF82DCF36D7C} Volume Shadow Copy WMI Provider
{AC48FFE0-F8C4-11d1-A030-00C04FB6809F} RequestMakeCall Class
{AED6483E-3304-11d2-86F1-006008B0E5D2} Video Render Dynamic Terminal
{AED6483F-3304-11d2-86F1-006008B0E5D2} Media Streaming Dynamic Terminal
{B138E92F-F502-4adc-89D9-134C8E580409} FileRecordingTerminal Class
{BB918E32-2A5C-4986-AB40-1686A034390A} Plug-in Terminal Class
{BCEA735B-4DAC-4B71-9C47-1D560AFD2A9B} DfsShellAdmin Class
{E9225296-C759-11d1-A02B-00C04FB6809F} DispatchMapper Class
{ECCDF543-45CC-11CE-B9BF-0080C87CDBA6} DfsShell Class
Tue Jul 14 04:54:26 2009 Z
{02A3586C-D264-40BF-97F7-FE40F7E3A882} Microsoft Virtual Disk Service Dynamic
Provider
{0B5A2C52-3EB9-470a-96E2-6C6D4570E40F} VssSnapshotMgmt Class
{135698D2-3A37-4d26-99DF-E2BB6AE3AC61} IVolumeClient3_PSFacy
{3A410F21-553F-11d1-8E5E-00A0C92C9D5D} IDMRremoteServer_PSFacy
{4BDAFC52-FE6A-11d2-93F8-00105A11164A} IVolumeClient2_PSFacy
{65EE1DBA-8FF4-4a58-AC1C-3470EE2F376A} VSSoftwareProvider Class
{7086AD76-44BD-11D0-81ED-00A0C90FC491} DiskManagement.UITasks
{7D1933CB-86F6-4A98-8628-01BE94C9A575} Virtual Disk Service
{80CB8C11-0E10-45F4-A1BA-EAD3838D7034} Microsoft Virtual Disk Service Virtual
Disk Provider
{8EAD3A12-B2C1-11d0-83AA-00A0C92C9D5D} DiskManagement.SnapInExtension
{95243A62-2F9B-4FDF-B437-40D965F6D17F} VSSRemoteCoordinator Class
{9C38ED61-D565-4728-AEEE-C80952F0ECDE} Virtual Disk Service Loader
{AEB84C83-95DC-11D0-B7FC-B61140119C4A} DiskManagement.Control
{D2D79DF5-3400-11d0-B40B-00AA005FF586} IVolumeClient_PSFacy
{D2D79DF7-3400-11d0-B40B-00AA005FF586} IDMNotify_PSFacy
{DBFCA500-8C31-11D0-AA2C-00A0C92749A3} DiskManagement.SnapInComponent
{DE010DA1-289B-4232-8CD0-5112DCA6A7B3} Microsoft Virtual Disk Service Basic
Provider
{DEB01010-3A37-4d26-99DF-E2BB6AE3AC61} IVolumeClient4_PSFacy
{E0393303-90D4-4A97-AB71-E9B671EE2729} VDS ProxyStub
{E13B6686-3F39-11D0-96F6-00A0C9191601} DiskManagement.SnapIn
{E13B6688-3F39-11D0-96F6-00A0C9191601} DiskManagement.DataObject
{E579AB5F-1CC4-44b4-BED9-DE0991FF0623} VSSCoordinator Class
{F2C2787D-95AB-40D4-942D-298F5F757874} PSFactoryBuffer
{FAC1D9C0-0296-11D1-A840-00A0C92C9D5D} DiskManagement.SnapInAbout
Tue Jul 14 04:54:25 2009 Z
{00020C01-0000-0000-C000-000000000046} Sound (OLE2)
{00022601-0000-0000-C000-000000000046} Media Clip
{00022602-0000-0000-C000-000000000046} Video Clip
{00022603-0000-0000-C000-000000000046} MIDI Sequence
{0003000C-0000-0000-C000-000000000046}
{0003000D-0000-0000-C000-000000000046} Sound
{0003000E-0000-0000-C000-000000000046} Media Clip

```

## SOFTWARE OUTPUT

```

{08d450b7-f7e5-4424-8229-11888adb7c14}
{0bf754aa-c967-445c-ab3d-d8fda9bae7ef} SlideshowContextMenu
{0CD7A5C0-9F37-11CE-AE65-08002B2E1262} Cabinet Shell Folder
{1a184871-359e-4f67-aad9-5b9905d62232} Microsoft Windows Font Context Menu
Handler
{299D0193-6DAA-11d2-B679-006097DF5BD4} FTP IDataObject impl
{35CEC8A3-2BE6-11D2-8773-92E220524153}
{4f6bcd94-c2a5-42ce-8dbc-31e794be4630} Shell Computer Accounts
{56EA1054-1959-467f-BE3B-A2A787C4B6EA} SHACCT Profile Notification Handler
{593FB605-4854-4965-B5A1-70AB54AB6475}
{596AB062-B4D2-4215-9F74-E9109B0A8153} Previous Versions Property Page
{59be4990-f85c-11ce-aff7-00aa003ca9f6} Shell extensions for Microsoft Windows
Network objects
{63da6ec0-2e98-11cf-8d82-444553540000} Microsoft FTP Folder
{68ddb56-9d1d-4fd9-89c5-c0da2a625392} UnexpectedShutdownReason
{730F6CDC-2C86-11D2-8773-92E220524153} SysTrayInvoker
{87CB4E0D-2E2F-4235-BC0A-7C62308011F6} PSFactoryBuffer
{888DCA60-FC0A-11CF-8F0F-00C04FD7D062} Compressed (zipped) Folder SendTo Target
{8a7cae0e-5951-49cb-bf20-ab3fa1e44b01} Windows Font previewer
{8E4062D9-FE1B-4b9e-AA16-5E8EEF68F48E} Registration Control
{8f3080a6-af99-4f2e-a806-f3d5702a0444} Shell Computer Groups
{93412589-74D4-4E4E-AD0E-E0CB621440FD} Font Settings
{987D8DFA-3E2C-4929-9C51-61AC8E00CBC3} Shell Logged On Accounts
{99CDC6E0-DA00-4dfa-8EB8-831D774F8891} Shell Profile Accounts
{9DB7A13C-F208-4981-8353-73CC61AE2783} Previous Versions
{a3c3d402-e56c-4033-95f7-4885e80b0111} Previous Versions Results Delegate Folder
{B6AFFB50-6F46-49B1-B912-C3F7A876CCCA}
{B8BE1E19-B9E4-4ebb-B7F6-A8FE1B3871E0} Microsoft Windows Font IExtractImage
Handler
{b8cdcb65-b1bf-4b42-9428-1dfdb7ee92af} Compressed (zipped) Folder Context Menu
{BD472F60-27FA-11cf-B8B4-444553540000} Compressed (zipped) Folder Right Drag
Handler
{BD84B380-8CA2-1069-AB1D-08000948F534} Microsoft Windows Font Folder
{C3C39131-B182-4801-B437-6D1E65B72F57} Shell User Accounts
{d20a3293-3341-4ae8-9aaf-8e397cb63c34} DefragEngine Class
{DFE49CFE-CD09-11D2-9643-00C04F79ADF0} Cabview Data Object
{E88DCCE0-B7B3-11d1-A9F0-00AA0060FA31} CompressedFolder
{ed9d80b9-d157-457b-9192-0e7280313bf0} Compressed (zipped) Folder DropHandler
{F20DA720-C02F-11CE-927B-0800095AE340} Package
{f8c2ab3b-17bc-41da-9758-339d7dbf2d88} Previous Versions Results Folder
{ff609cc7-d34d-4049-a1aa-2293517ffcc6} SetBackgroundContextMenu
Tue Jul 14 04:54:24 2009 Z
{0b2c9183-c9fa-4c53-ae21-c900b0c39965} CLSID_PathCompleteProvider
{1685D4AB-A51B-4af1-A4E5-CEE87002431D} CLSID_GrepProvider
{1C0F439D-7C29-4bde-8952-4EEB6A49E048} CLSID_GrepWdsResolver
{25256c24-3b75-49b3-a433-4bb2f8865896} CLSID_StartMenuProvider
{30276b4f-f25c-457c-a4b7-08574f8ea528} CLSID_ResultSetFactory
{36a479ef-8b67-4d01-8dda-753cfcb2dd96} CLSID_FilteredItemFactory

```

## SOFTWARE OUTPUT

```

{3722c3b1-82e8-4022-8b27-1f8a68b44ac7} CLSID_ProviderConfig
{3B1B5147-715E-49e0-AE9F-ADF86724BB89} CLSID_DateTimeIntervalGenerator
{3EA48300-8CF6-101B-84FB-666CCB9BCD32} OLE Docfile Property Page
{48E277F6-4E74-4cd6-BA6F-FA4F42898223} Windows Search OpenSearch Provider
{4A8ECCAC-181D-4c1b-BF8F-5D52C4008FB9} Accessing Options for Structured Query
{4db26476-6787-4046-b836-e8412a9e8a27} Shared Bitmap Object
{50EF4544-AC9F-4A8E-B21B-8A26180DB13F} Local Thumbnail Cache
{7988B571-EC89-11cf-9C00-00AA00A14F56} Microsoft Disk Quota
{7988B573-EC89-11cf-9C00-00AA00A14F56} Microsoft Disk Quota UI
{7efc002a-071f-4ce7-b265-f4b4263d2fd2} Local Thumbnail Cache
{807e5a10-4856-4f9a-8e3c-a1f7e75648b3} CLSID_QueryResult
{8099904b-0b91-4906-a89d-11de2bd8f737} StartMenu Path Complete Query Cache
{889900c3-59f3-4c2f-ae21-a409ea01e605} Shared Bitmap Object
{96B9DAE3-CF15-45e9-9719-57285348225E} Windows Search OpenSearch Icon Handler
{AB8902B4-09CA-4bb6-B78D-A8F59079A8D5} Thumbnail Cache Class Factory for Out of
Proc Server.
{BD84B381-8CA2-1069-AB1D-08000948F534} PANOSE Core Mapper
{daf95313-e44d-46af-be1b-cbacea2c3065} CLSID_StartMenuProviderFolder
{db6efb73-5153-43b7-8078-c6ffc4c0238c} CLSID_CheckCompositionCycles
{e345f35f-9397-435c-8f95-4e922c26259e} CLSID_StartMenuPathCompleteProviderFolder
Tue Jul 14 04:54:23 2009 Z
{05d7b0f4-2121-4eff-bf6b-ed3f69b894d7} Taskbar Control Panel
{05d7b0f4-2121-4eff-bf6b-ed3f69b894d8}
{05d7b0f4-2121-4eff-bf6b-ed3f69b894d9} Taskbar
{15fc1bac-8d83-4e87-8cc2-a70c9f66f943}
{17cd9488-1228-4b2f-88ce-4298e93e0966} Set User Defaults
{1968106d-f3b5-44cf-890e-116fcb9ecef1} Application Registration UI
{25EC352E-72E1-4724-9A28-4AE730072149}
{29D365AE-D23B-4004-8658-5ED2A59CD77C} Shell User Enumeration Object
{2B6DA137-316E-458B-A0AB-BE48C8EC39B9} Display Control Panel
{42071712-76d4-11d1-8b24-00a0c9068ff3} Display Adapter CPL Extension
{42071713-76d4-11d1-8b24-00a0c9068ff3} Display Monitor CPL Extension
{430da762-8632-4840-bc61-3eeaa078e62e} Windows Display Settings Data
{4345A2F4-05F5-48D6-B8A2-99D4A2E7B950} PSFactoryBuffer
{5BE4911E-3D99-4546-898D-7EE70201C519} Shell User Object
{5D05A4EB-54EA-4B7F-A28D-CE51F6BCBAF2} Virtual Factory for Display
{60632754-c523-4b62-b45c-4172da012619} User Accounts
{6C8EEC18-8D75-41B2-A177-8831D59D2D50} Mouse Control Panel
{725BE8F7-668E-4C7B-8F90-46BDB0936430} Keyboard Control Panel
{9b4e5207-9539-4258-b4a0-4e70e9e565ec} User Accounts Control Panel
{9C60DE1E-E5FC-40f4-A487-460851A8D915} AutoPlay
{C555438B-3C23-4769-A71F-B6D3D9B6053A} Display
{C6D7AB70-3D91-433D-8D9E-E1B52035C47F}
{CE510457-55EC-4f86-91BE-323BC91AC34F} Shell User Domain Enumeration Object
{D4EFF9CD-16DE-446e-83C5-9537543CF4A1} Set User Defaults Control Panel
{f92e8c40-3d33-11d2-b1aa-080036a75b03} Display Troubleshoot CPL Extension
Tue Jul 14 04:54:22 2009 Z
{00A77FF7-A514-493e-B721-CDF8CB0F5B59} Computer Info Advise

```



## SOFTWARE OUTPUT

```

{025A5937-A6BE-4686-A844-36FE4BEC8B6D} Power Options
{0289a7c5-91bf-4547-81ae-fec91a89dec5} Microsoft Windows Remote Shell Host
{03C93300-8AB2-41C5-9B79-46127A30E148} PSFactoryBuffer
{045473BC-A37B-4957-B144-68105411ED8E} PSFactoryBuffer
{047DEC5A-95C1-4C86-827F-7B8C92EBA67A} PSFactoryBuffer
{0ce3e86f-d5cd-4525-a766-1abab1a752f5} SideShowNotification Class
{1C749B87-568C-4865-8E73-6413F8372CE6} Lpksetup LUA Elevation
{2aa2b5fe-b846-4d07-810c-b21ee45320e3} Network Provisioning via XML Class
{2EA7A549-7BFF-4aae-BAB0-22D43111DE49} PSFactoryBuffer
{3F66389B-BA65-4782-BA9D-B66367C8E7F1} Power Control Panel
{45FD65ED-6BC2-47ae-B391-9E2B79F07C52} System Control Panel
{500DD1A1-B32A-4a37-9283-1185FB613899} PSFactoryBuffer
{514B5E31-5596-422F-BE58-D804464683B5} Region and Language UAC Elevation
{5BFF4E02-D379-4050-A382-C6504A980D46} PowrProfApi
{62D8ED13-C9D0-4CE8-A914-47DD628FB1B0} Region and Language
{7A076CE1-4B31-452a-A4F1-0304C8738100} Network and Sharing Center Cpl Elevated
Virtual Factory
{7C92505F-53A4-4D39-B31C-871D82A907DE} PSFactoryBuffer
{7DE087A5-5DCB-4df7-BB12-0924AD8FBD9A} WSMAN InternalAutomation Class
{84CCE1D2-97AD-4448-AF0F-A79164073A60} Personalization Control Panel Element
Provider
{8E908FC9-BECC-40f6-915B-F4CA0E70D03D} Network and Sharing Center
{90954C68-4D60-4023-A1F8-C6AF6F62E1C8} Network and Sharing Center
{9678f47f-2435-475c-b24a-4606f8161c16} Microsoft Windows WSMAN Provider Host
{98068995-54d2-4136-9bc9-6dbcb0a4683f} Microsoft Windows Remote Shell Host With
User Settings
{9A7C3FC6-8C9E-40A8-8CD9-0F3715483825} PSFactoryBuffer
{9acf41ed-d457-4cc1-941b-ab02c26e4686} Microsoft Windows WSMAN Provider Host With
User Settings
{9df523b0-a6c0-4ea9-b5f1-f4565c3ac8b8} Date and Time Properties
{a323554a-0fe1-4e49-aeel-6722465d799f} DateTimeCPL Flyout Class
{BA9BB214-D930-4206-8F8F-BF0F1EAA4A6B} PSFactoryBuffer
{BB06C0E4-D293-4f75-8A90-CB05B6477EEE} System
{BBD8C065-5E6C-4e88-BFD7-BE3E6D1C063B} Virtual Factory for Power Options Control
Panel
{BCED617B-EC03-420b-8508-977DC7A686BD} WSMAN Automation Class
{BF85540E-0DF3-47bc-AC5D-305442704708}
{C0DCC3A6-BE26-4bad-9833-61DFACE1A8DB} Network Center LUA
{c89e334c-e65f-4156-842e-ea89cec71dea} WFP and IPsec Helper Class
{DFBBDBF8-18DE-49b8-83DC-EBC727C62D94} SideShowKeyCollection Class
{e20543b9-f785-4ea2-981e-c4ffa76bbc7c} SideShowSession Class
{E2E7934B-DCE5-43C4-9576-7FE4F75E7480} Date and Time Control Panel
{E640F415-539E-4923-96CD-5F093BC250CD} SideShowPropVariantCollection Class
{f6b13ba7-d626-45e5-82c5-26e596114dc0} WFP Clients Extensible Helper Class
{F73C1438-71B4-4D91-AD13-1F889A03AC67} PSFactoryBuffer
Tue Jul 14 04:54:21 2009 Z
{01D0A625-782D-4777-8D4E-547E6457FAD5} CEIPLuaElevationHelper
{0E3BE0D7-030E-4CA3-A911-D86E24AE0A3C} TCImeComponentMgr

```

## SOFTWARE OUTPUT

```

{0E4EFFC0-2387-11D3-B372-00105A98B7CE} Microsoft.JScript.JSAuthor
{0E9A7BB5-F699-4D66-8A47-B919F5B6A1DB} ERC Lua Support
{11D5C91F-0A98-11D1-BB10-00C04FC9A3A3} Computer Management 1.0 Object
{17A898FB-3FC5-455C-87A9-DB06F9D0A557} ImeCommonAPIClassFactory
{1C5346B8-63E1-4c2b-B125-3C5DB94E946C} TC IME7 Dictionary Applet
{20cd9315-87d0-40b4-b925-0a8f208e1f8d} ImeCommonAPI_KOR_Desktop_V1 Class
{20D04FE0-3AEA-1069-A2D8-08002B30309D} Computer
{227188db-3179-4fdf-af3a-da3b85a0b3cc} ImeCommonAPIClassFactory_KOR_Desktop_V1
Class
{25ECF786-A925-4706-A269-EEF5AD6899DB} ImeCommonAPIClassFactory
{432D76CE-8C9E-4EED-ADDD-91737F27A8CB} Microsoft.JScript.DebugConvert
{49FC0B81-206C-407F-9F5B-106E5A3EE2D7} SCImeComponentMgr
{4BC67F23-D805-4384-BCA3-6F1EDFF50E2C} ERCLuaElevationHelper
{50055B2F-D4FF-42E1-9D8F-5D48F327F3AC} WERCOM
{531FDEBF-9B4C-4A43-A2AA-960E8FCDC732} ImTCTip
{58221C67-EA27-11CF-ADCF-00AA00A80033} Computer Management 1.0 Object
{6A02951C-B129-4D26-AB92-B9CA19BDCA26} Microsoft.JScript.COMPropertyInfo
{81D4E9C9-1D3B-41BC-9E6C-4B40BF79E35E} ImSCTip
{8D9B1EC0-181B-4d6d-987E-2754B506B242} MS PinYin 5.0 Dictionary Applet
{95688ffa-250d-49bd-b40a-8ed3a8ef4c8e} ImeKeyEventHandler Class
{A028AE76-01B1-46C2-99C4-ACD9858AE02F} IMKRTIP
{B71E484D-93ED-4B56-BFB9-CEED5134822B} Microsoft.JScript.Vsa.VsaEngine
{C3A43F75-FE02-47d8-B3EE-0B568C0C5043}
{C7B9C313-2FD4-4384-8571-7ABC08BD17E5} Microsoft.JScript.COMMethodInfo
{CA0F511A-FAF2-4942-B9A8-17D5E46514E8} Microsoft.JScript.COMFieldInfo
{CA236752-2E77-4386-B63B-0E34774A413D}
{CACA7238-3C7E-4a25-AD73-DE1A4F8C7214}
{D01B8F28-0BD1-4652-A415-8229F5EE506C} PSFactoryBuffer
{D74A07B1-EA36-4f32-A85A-9777A4AE12AA} PSFactoryBuffer
{F407D01A-0BCB-4591-9BD6-EA4A71DF0799} CHT Language model
Tue Jul 14 04:54:20 2009 Z
{0095b496-f121-4256-96a0-09179828cc16} CImeProductObject_JK Class
{019F7150-E6DB-11D0-83C3-00C04FDD8B2E} Microsoft IME (Japanese)
{01FE4A1F-CC5C-44AB-A1E6-CFBD9249146D} PSFactoryBuffer
{03B5835F-F03C-411B-9CE2-AA23E1171E36} IMJPTIP
{17fb3711-de14-477f-8b81-32a9c11a6938} CImeCommonAPI Class
{35CC8486-4FB1-11D3-A5DA-00C04F88249B} Microsoft Korean IME HandWriting Applet
{3A59A18B-F03C-48CB-8AA7-181D35291FD7} IIMECheckDefaultInputProfile
{4BE5C3B3-53A2-4F2F-AF9D-D26A5327EB92} Microsoft Korean IME 8.0 SKF Applet
{4C870C20-4ED3-4235-9A2A-7185F8A87D06} HanjaDic Class
{6279B7CB-D768-4FBE-A6D5-ADD4F711E53B} Microsoft IME SingleKanjiDictionary
interface
{6A91029E-AA49-471B-AEE7-7D332785660D} Microsoft IME (Japanese)
{6bdadf65-eb94-419b-907c-0ba9dda7f0df} CImeRequestSender_JK Class
{6ffa842b-fd90-4a0e-9315-21c52b2457aa} CImeKeyMapView_JK Class
{88c524ca-551b-4c01-9a42-cdb16b745291} ImeCommonAPI_JPN_Desktop_V1 Class
{8F0A1029-0DF8-4765-A5FD-16E8ECB3545C} PSFactoryBuffer
{91162401-6E6B-478A-A7FF-994EBA35B9C3} PSFactoryBuffer

```

## SOFTWARE OUTPUT

```

{99a73266-0cdf-4479-88af-1842cbaada22} IImeIPointSrv wrapper class
{9f75fdc4-0aba-4866-88a9-75ebb9e7d584} CImeCommandAvailabilityView_JK Class
{9FF13758-469B-45A8-8CC7-72182BD7E9BA} Microsoft IME SKF Applet
{a38f3677-32fc-4dac-99b3-d804b193d2c4} ImeKeyEventHandler Class
{A8C3476D-20E1-4d56-96E7-84E24952228B} UserDicManager Class
{af9d2278-060f-4a17-99a9-5044f7f843a8} CImeProperty_JK Class
{D26C7A0A-83A0-48D3-9174-529DB999B4A4} PSFactoryBuffer
{d54e0450-f515-42ac-bf22-b254a2764d49}
{DD5CF606-9EA7-49E1-8E82-B789E4443B4F} MS-IME HandWriting Applet
{e126b7dd-1c3b-4821-b861-a6da9ce6f096} ImeCommonAPIClassFactory_JPN_Desktop_V1
Class
Tue Jul 14 04:54:19 2009 Z
{414AC301-8D95-43C8-99D0-3F25E4076945} Microsoft Shared Correction UI
{A3037D66-C043-4F54-91A0-2CDB642E7718} IMETip
{CCB1D8CB-D39F-41C9-B793-0196214BDC4E} IMECFM
Tue Jul 14 04:54:14 2009 Z
{FD5CD8B1-6FE0-44F3-BBFB-65E3655B096E}
{FEDB2179-2335-48F1-AA28-5CDA35A2B36D}
Tue Jul 14 04:54:13 2009 Z
{00B01B2E-B1FE-33A6-AD40-57DE8358DC7D} System.Security.Cryptography.HMACSHA1
{01FF4E4B-8AD0-3171-8C82-5C2F48B87E3D}
System.Runtime.Remoting.Metadata.SoapMethodAttribute
{026CC6D7-34B2-33D5-B551-CA31EB6CE345} System.Collections.SortedList
{047a9a40-657e-11d3-8d5b-00104b35e7ef} Microsoft Common Language Runtime Debugger
Publisher
{05EBA309-0164-11D3-8729-00C04F79ED0D} Cor IE Security Manager,
CorIESecurityManager, CorIESecurityManager 1
{06B81C12-A5DA-340D-AFF7-FA1453FBC29A}
System.Security.Policy.AllMembershipCondition
{07F94112-A42E-328B-B508-702EF62BCC29}
System.Runtime.InteropServices.COMException
{08295C62-7462-3633-B35E-7AE68ACA3948} System.ObsoleteAttribute
{09A60795-31C0-3A79-9250-8D93C74FE540}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapInteger
{0A29FF9E-7F9C-4437-8B11-F424491E3931} NDP SymBinder
{0A3976C5-4529-4ef8-B0B0-42EED37082CD} NDP SymReader
{0AE2DEB0-F901-478b-BB9F-881EE8066788} NDP SymWriter
{0D23F8B4-F2A6-3EFF-9D37-BDF79AC6B440} System.Reflection.TargetException
{0D52ABE3-3C93-3D94-A744-AC44850BACCD}
System.Collections.Generic.KeyNotFoundException
{0E71F9BD-C109-3352-BD60-14F96D56B6F3}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNormalizedString
{0FF66430-C796-3EE7-902B-166C402CA288} System.MemberAccessException
{108296C1-281E-11D3-BD22-0000F80849BD} Pdb based CorSymWriter
{112BC2E7-9EF9-3648-AF9E-45C0D4B89929} System.TypeLoadException
{11581718-2434-32E3-B559-E86CE9923744} System.OperationCanceledException
{1163D0CA-2A02-37C1-BF3F-A9B9E9D49245}
System.Runtime.Remoting.Proxies.ProxyAttribute

```

## SOFTWARE OUTPUT

```

{146855FA-309F-3D0E-BB3E-DF525F30A715} System.Collections.Hashtable
{146A47AB-A2CF-3587-BB25-2B286D7566B4} System.Globalization.NumberFormatInfo
{14910622-09D4-3B4A-8C1E-9991DBDCC553} System.Diagnostics.StackFrame
{14BE6B21-C682-3A3A-8B24-FEE75B4FF8C5}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNmtokens
{18B1C7EE-68E3-35BB-9E40-469A223285F7}
System.Runtime.Serialization.OnDeserializedAttribute
{1A06A4DC-E239-3717-89E1-D0683F3A5320} System.Globalization.KoreanCalendar
{1B979846-AAEB-314B-8E63-D44EF1CB9EFC}
System.Diagnostics.DebuggerStepperBoundaryAttribute
{1C97EF1D-74ED-3D21-84A4-8631D959634A}
System.Runtime.Serialization.OptionalFieldAttribute
{1D09B407-A97F-378A-ACCB-82CA0082F9F3}
System.Runtime.Hosting.ApplicationActivator
{1E66F26B-79EE-11D2-8710-00C04F79ED0D} Cor MIME Filter, CorFltr, CorFltr 1
{1F17C39C-99D5-37E0-8E98-8F27044BD50A}
System.Security.Cryptography.DSASignatureDeformatter
{1F9F18A3-EFC0-3913-84A5-90678A4A9A80}
System.Security.Cryptography.RijndaelManaged
{20051D1B-321F-3E4D-A3DA-5FBE892F7EC5} System.Security.Cryptography.HMACRIPEMD160
{204D5A28-46A0-3F04-BD7C-B5672631E57F}
System.Runtime.InteropServices.PreserveSigAttribute
{21F5A790-53EA-3D73-86C3-A5BA6CF65FE9} System.Runtime.Remoting.ObjRef
{2206D773-CA1C-3258-9456-CEB7706C3710} System.Globalization.HebrewCalendar
{24540EBC-316E-35D2-80DB-8A535CAF6A35} System.Runtime.Remoting.RemotingException
{24800CD0-0F4E-4df7-9F69-3C6903C89224} Microsoft Visual Basic Scripting Engine
{24EEC005-3938-3C71-821D-7F68FD850B2D}
System.Runtime.Remoting.Messaging.RemotingSurrogateSelector
{2763BE6B-F8CF-39D9-A2E8-9E9815C0815E}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapIdrefs
{27E986E1-BAEC-3D48-82E4-14169CA8CECF}
System.Threading.ThreadInterruptedException
{27F31D55-D6C6-3676-9D42-C40F3A918636} System.IO.StringWriter
{2846AE5E-A9FA-36CF-B2D1-6E95596DBDE7} System.Reflection.AmbiguousMatchException
{29625281-51CE-3F8A-AC4D-E360CACB92E2}
System.Diagnostics.DebuggerNonUserCodeAttribute
{29A6CF6F-D663-31A7-9210-1347871681FC}
System.Security.Permissions.GacIdentityPermission
{29C69707-875F-3678-8F01-283094A2DFB1} System.CannotUnloadAppDomainException
{29C98DFC-AC6B-4788-BDDD-CA41D6D3704A} Dia based SymReader
{2BB6C5E0-C2B9-3608-8868-21CFD6DDB91E}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNonPositiveInteger
{2C314899-8F99-3041-A49D-2F6AFC0E6296} System.Security.Cryptography.HMACSHA256
{2D5EC63C-1B3E-3EE4-9052-EB0D0303549C}
System.Runtime.InteropServices.SafeArrayTypeMismatchException
{2DECBCB7-BAC0-316D-9131-43035C5CB480}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapDate
{30AC0B94-3BDB-3199-8A5D-ECA0C5458381}

```

## SOFTWARE OUTPUT

System.Runtime.Serialization.OnDeserializingAttribute  
 {31C967B5-2F8A-3957-9C6D-34A0731DB36C} System.Globalizatio.StringInfo  
 {31D353B3-0A0A-3986-9B20-3EC4EE90B389}  
 System.EnterpriseServices.Internal.ServerWebConfig  
 {346D5B9F-45E1-45C0-AADF-1B7D221E9063}  
 System.EnterpriseServices.Internal.SoapClientImport  
 {3495E5FA-2A90-3CA7-B3B5-58736C4441DD} System.ParamArrayAttribute  
 {35E946E4-7CDA-3824-8B24-D799A96309AD} System.Collections.CaseInsensitiveComparer  
 {36DCDA30-DC3B-4D93-BE42-90B2D74C64E7}  
 System.EnterpriseServices.RegistrationConfig  
 {374050DD-6190-3257-8812-8230BF095147} System.Globalizatio.JapaneseCalendar  
 {390E92C9-FA66-3357-BEF2-45A1F34186B9}  
 System.Security.Policy.GacMembershipCondition  
 {39B68485-6773-3C46-82E9-56D8F0B4570C} System.Security.Cryptography.MACTripleDES  
 {3B0398C9-7812-4007-85CB-18C771F2206F}  
 System.EnterpriseServices.Internal.ComManagedImportUtil  
 {3BD1F243-9BC4-305D-9B1C-0D10C80329FC} System.ArgumentNullException  
 {3C9DCA8B-4410-3143-B801-559553EB6725} System.Text.UTF7Encoding  
 {3CDED51A-86B4-39F0-A12A-5D1FDCED6546}  
 System.Runtime.Remoting.RemotingTimeoutException  
 {3D367908-928F-3C13-8B93-5E1718820F6D}  
 System.Security.Cryptography.RIPEMD160Managed  
 {3DDB2114-9285-30A6-906D-B117640CA927}  
 System.Security.Policy.ApplicationDirectoryMembershipCondition  
 {3E5509F0-1FB9-304D-8174-75D6C9AFE5DA} System.Threading.ThreadStateException  
 {3E8E0F03-D3FD-3A93-BAE0-C74A6494DBCA} System.AppDomainSetup  
 {3F4A4283-6A08-3E90-A976-2C2D3BE4EB0B} System.Reflection.AssemblyNameProxy  
 {3FA7A1C5-812C-3B56-B957-CB14AF670C09}  
 System.Security.Cryptography.SignatureDescription  
 {3FB717AF-9D21-3016-871A-DF817ABDDD51} System.EventArgs  
 {3FDCEEC6-B14B-37E2-BB69-ABC7CA0DA22F} System.ArgumentException  
 {40031115-09D2-3851-A13F-56930BE48038}  
 System.Security.Cryptography.RNGCryptoServiceProvider  
 {405C2D81-315B-3CB0-8442-EF5A38D4C3B8} System.Diagnostics.StackTrace  
 {40AE2088-CE00-33AD-9320-5D201CB46FC9}  
 System.Diagnostics.SymbolStore.SymDocumentType  
 {41970D73-92F6-36D9-874D-3BD0762A0D6F} System.Diagnostics.DebuggerHiddenAttribute  
 {4224AC84-9B11-3561-8923-C893CA77ACBE} System.SystemException  
 {4286FA72-A2FA-3245-8751-D4206070A191} System.OverflowException  
 {433CA926-9887-3541-89CC-5D74D0259144}  
 System.Runtime.Remoting.Metadata.W3cXsd2001.SoapIdref  
 {43CD41AD-3B78-3531-9031-3059E0AA64EB} System.Version  
 {44181B13-AE94-3CFB-81D1-37DB59145030} System.Security.Cryptography.SHA256Managed  
 {4479C009-4CC3-39A2-8F92-DFCDF034F748}  
 System.IO.IsolatedStorage.IsolatedStorageException  
 {458AA3B5-265A-4B75-BC05-9BEA4630CF18}  
 System.EnterpriseServices.Internal.AssemblyLocator  
 {4599202D-460F-3FB7-8A1C-C2CC6ED6C7C8} System.Collections.Stack

## SOFTWARE OUTPUT

```

{46080CA7-7CB8-3A55-A72E-8E50ECA4D4FC}
System.Runtime.CompilerServices.CallConvThiscall
{463AE13F-C7E5-357E-A41C-DF8762FFF85C}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapMonthDay
{46E97093-B2EC-3787-A9A5-470D1A27417C} System.DllNotFoundException
{475E398F-8AFA-43A7-A3BE-F4EF8D6787C9}
System.Runtime.InteropServices.RegistrationServices
{477A7D8E-8D26-3959-88F6-F6AB7E7F50CF} System.Security.Cryptography.HMACSHA512
{47D3C68D-7D85-3227-A9E7-88451D6BADFC}
System.Collections.CaseInsensitiveHashCodeProvider
{48728B3F-F7D9-36C1-B3E7-8BF2E63CE1B3}
System.Runtime.Remoting.Channels.TransportHeaders
{48A75519-CB7A-3D18-B91E-BE62EE842A3E}
System.Threading.SynchronizationLockException
{48AD62E8-BD40-37F4-8FD7-F7A17478A8E6}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapDateTime
{48C6E96F-A2F3-33E7-BA7F-C8F74866760B} System.IO.FileNotFoundException
{48D0CFE7-3128-3D2C-A5B5-8C7B82B4AB4F}
System.Runtime.CompilerServices.MethodImplAttribute
{4B601364-A04B-38BC-BD38-A18E981324CF}
System.Runtime.CompilerServices.CompilerGlobalScopeAttribute
{4BE89AC3-603D-36B2-AB9B-9C38866F56D5}
System.Runtime.InteropServices.SafeArrayRankMismatchException
{4C3EBFD5-FC72-33DC-BC37-9953EB25B8D7} System.AccessViolationException
{4C69C54F-9824-38CC-8387-A22DC67E0BAB}
System.Security.Cryptography.X509Certificates.X509Certificate
{4D187AC2-D815-3B7E-BCEA-8E0BBC702F7C}
System.Security.Cryptography.RSAOAEPKeyExchangeDeformatter
{4E515531-7A71-3CDD-8078-0A01C85C8F9D}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapName
{4E77EC8F-51D8-386C-85FE-7DC931B7A8E7} System.Random
{4F272C37-F0A8-350C-867B-2C03B2B16B80}
System.Runtime.Serialization.ObjectIDGenerator
{50369004-DB9A-3A75-BE7A-1D0EF017B9D3}
System.Runtime.Serialization.Formatters.Binary.BinaryFormatter
{50AAD4C2-61FA-3B1F-8157-5BA3B27AEE61} System.STAThreadAttribute
{53A3C917-BB24-3908-B58B-09ECDA99265F}
System.Runtime.Remoting.InternalRemotingServices
{5520B6D3-6EC6-3CE7-958B-E69FAF6EFF99}
System.Runtime.Remoting.Contexts.SynchronizationAttribute
{5610F042-FF1D-36D0-996C-68F7A207D1F0}
System.Security.AllowPartiallyTrustedCallersAttribute
{57154C7C-EDB2-3BFD-A8BA-924C60913EBF}
System.Runtime.Serialization.SerializationException
{58897D76-EF6C-327A-93F7-6CD66C424E11} System.MissingMethodException
{58D052BC-A3DF-3508-AC95-FF297BDC9F0C} System.IO.EndOfStreamException
{590E4A07-DAFC-3BE7-A178-DA349BBA980B}
System.Runtime.CompilerServices.IUnknownConstantAttribute

```

## SOFTWARE OUTPUT

```

{5A18D43E-115B-3B8B-8245-9A06B204B717}
System.Diagnostics.SymbolStore.SymLanguageType
{5B76534C-3ACC-3D52-AA61-D788B134ABE2}
System.Runtime.Remoting.Metadata.SoapFieldAttribute
{5C35F099-165E-3225-A3A5-564150EA17F5}
System.Runtime.Remoting.Channels.ServerChannelSinkStack
{5C3E6CE8-B218-3762-883C-91BC987CDC2D} System.Globalization.JulianCalendar
{5CA9971B-2DC3-3BC8-847A-5E6D15CBB16E} System.IndexOutOfRangeException
{5F3A0F8D-5EF9-3AD5-94E0-53AFF8BCE960}
System.Security.Cryptography.ToBase64Transform
{5F9A955F-AA55-4127-A32B-33496AA8A44E}
System.EnterpriseServices.Internal.SoapUtility
{61B3E12B-3586-3A58-A497-7ED7C4C794B9} System.AppDomainUnloadedException
{62545937-20A9-3D0F-B04B-322E854EACB0} System.Security.Policy.Evidence
{62E92675-CB77-3FC9-8597-1A81A5F18013}
System.Security.Cryptography.RC2CryptoServiceProvider
{630A3EF1-23C6-31FE-9D25-294E3B3E7486}
System.Runtime.InteropServices.ComRegisterFunctionAttribute
{647053C3-1879-34D7-AE57-67015C91FC70} System.ArithmeticException
{6619A740-8154-43BE-A186-0319578E02DB} PSFactoryBuffer
{66CE75D4-0334-3CA6-BCA8-CE9AF28A4396} System.FlagsAttribute
{673DFE75-9F93-304F-ABA8-D2A86BA87D7C}
System.Security.Cryptography.DSACryptoServiceProvider
{676E1164-752C-3A74-8D3F-BCD32A2026D6} System.ArrayTypeMismatchException
{682D63B8-1692-31BE-88CD-5CB1F79EDB7B} System.ApplicationException
{6850404F-D7FB-32BD-8328-C94F66E8C1C7}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNonNegativeInteger
{6896B49D-7AFB-34DC-934E-5ADD38EEEE39} System.Collections.ArrayList
{68F8AEA9-1968-35B9-8A0E-6FDC637A4F8E} System.Globalization.GregorianCalendar
{6C1C243A-2146-3342-8078-AC4BFB9DB4E9}
System.EnterpriseServices.CompensatingResourceManager.ClerkMonitor
{6F674828-9081-3B45-BC39-791BD84CCF8F}
System.Security.Cryptography.RSAPKCS1SignatureDeformatter
{6F8527BF-5AAD-3236-B639-A05177332EFE}
System.Runtime.Serialization.OnSerializedAttribute
{6FEF44D0-39E7-4C77-BE8E-C9F8CF988630} Microsoft Common Language Runtime Debugger
{70A738D1-1BC5-3175-BD42-603E2B82C08B} System.Globalization.DateTimeFormatInfo
{726BBDF4-6C6D-30F4-B3A0-F14D6AEC08C7}
System.Resources.MissingManifestResourceException
{742AD1FB-B2F0-3681-B4AA-E736A3BCE4E1}
System.Runtime.InteropServices.MarshalDirectiveException
{74BDD0B9-38D7-3FDA-A67E-D404EE684F24} System.ArgumentOutOfRangeException
{75215200-A2FE-30F6-A34B-8F1A1830358E} System.UnauthorizedAccessException
{75999EBA-0679-3D43-BDC4-02E4D637F1B1}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapYear
{769B8B68-64F7-3B61-B744-160A9FCC3216} System.Globalization.TaiwanCalendar
{777F668E-3272-39CD-A8B5-860935A35181}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapToken

```

## SOFTWARE OUTPUT

```

{78D22140-40CF-303E-BE96-B3AC0407A34D}
System.Runtime.InteropServices.RuntimeEnvironment
{7AE01D6C-BEE7-38F6-9A86-329D8A917803}
System.Security.SuppressUnmanagedCodeSecurityAttribute
{7AE844F0-ECA8-3F15-AE27-AFA21A2AA6F8}
System.Security.Cryptography.PKCS1MaskGenerationMethod
{7B769B29-35F0-3BDC-AAE9-E99937F6CDEC}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapPositiveInteger
{7B938A6F-77BF-351C-A712-69483C91115D}
System.Reflection.InvalidFilterCriteriaException
{7BC115CD-1EE2-3068-894D-E3D3F7632F40}
System.Security.Cryptography.RSAPKCS1SignatureFormatter
{7E3393AB-2AB2-320B-8F6F-EAB6F5CF2CAF} System.Security.UnverifiableCodeAttribute
{7E34AB89-0684-3B86-8A0F-E638EB4E6252} System.NotFiniteNumberException
{7F6BCBE5-EB30-370B-9F1B-92A6265AFEDD} System.InvalidCastException
{7F71DB2D-1EA0-3CAE-8087-26095F5215E6} System.NullReferenceException
{7F8C7DC5-D8B4-3758-981F-02AF6B42461A}
System.Security.Cryptography.CryptographicException
{7F976B72-4B71-3858-BEE8-8E3A3189A651} System.Collections.Queue
{7FD3958D-0A14-3001-8074-0D15EAD7F05C} System.Security.Cryptography.SHA384Managed
{7FE87A55-1321-3D9F-8FEF-CD2F5E8AB2E9} System.Threading.Overlapped
{81C5FE01-027C-3E1C-98D5-DA9C9862AA21} System.Object
{837A6733-1675-3BC9-BBF8-13889F84DAF4}
System.Runtime.CompilerServices.DiscardableAttribute
{84589833-40D7-36E2-8545-67A92B97C408} System.Security.HostSecurityManager
{84F70B6C-D59E-394A-B879-FFCC30DDCAA2}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapLanguage
{8833BC41-DC6B-34B9-A799-682D2554F02F} System.IO.DirectoryNotFoundException
{88C8A919-EB24-3CCA-84F7-2EA82BB3F3ED}
System.Runtime.Serialization.SurrogateSelector
{89A86E7B-C229-4008-9BAA-2F5C8411D7E0}
System.EnterpriseServices.RegistrationHelper
{89BCC804-53A5-3EB2-A342-6282CC410260} System.SerializableAttribute
{89D26277-8408-3FC8-BD44-CF5F0E614C82} System.Security.Policy.PolicyException
{8A3FD229-B2A9-347F-93D2-87F3B7F92753}
System.Runtime.InteropServices.ComConversionLossAttribute
{8C1425C9-A7D3-35CD-8248-928CA52AD49B}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapHexBinary
{8C40D44A-4EDE-3760-9B61-50255056D3C7} System.Text.UTF8Encoding
{8D36569B-14D6-3C3D-B55C-9D02A45BFC3D} System.MissingFieldException
{8F45C7FF-1E6E-34C1-A7CC-260985392A05}
System.Runtime.InteropServices.ComUnregisterFunctionAttribute
{8F6D198C-E66F-3A87-AA3F-F885DD09EA13}
System.Security.Cryptography.DSASignatureFormatter
{8FD730C1-DD1B-3694-84A1-8CE7159E266B}
System.Runtime.Remoting.Lifetime.LifetimeServices
{91591469-EFEF-3D63-90F9-88520F0AA1EF} System.InvalidProgramException
{9173D971-B142-38A5-8488-D10A9DCF71B0} System.Threading.ReaderWriterLock

```



## SOFTWARE OUTPUT

{91F672A3-6B82-3E04-B2D7-BAC5D6676609} System.Diagnostics.Debugger  
 {92755472-2059-3F96-8938-8AC767B5187B}  
 System.Security.Cryptography.RSAPKCS1KeyExchangeFormatter  
 {92E76A74-2622-3AA9-A3CA-1AE8BD7BC4A8} System.MethodAccessException  
 {93D11DE9-5F6C-354A-A7C5-16CCA64A9B8} System.Reflection.ObfuscationAttribute  
 {93F551D6-2F9E-301B-BE63-85AEF508CAE0}  
 System.Diagnostics.DebuggerStepThroughAttribute  
 {9546306B-1B68-33AF-80DB-3A9206501515} System.InvalidOperationException  
 {964AA3BD-4B12-3E23-9D7F-99342AF8E812} System.FormatException  
 {96705EE3-F7AB-3E9A-9FB2-AD1D536E901A} System.ContextStaticAttribute  
 {96A058CD-FAF7-386C-85BF-E47F00C81795} System.Runtime.InteropServices.InAttribute  
 {9A3A64F4-8BA5-3DCF-880C-8D3EE06C5538}  
 System.Runtime.Remoting.Metadata.W3cXsd2001.SoapEntities  
 {9A944885-EDAF-3A81-A2FF-6A9D5D1ABFC7}  
 System.Runtime.InteropServices.InvalidOleVariantTypeException  
 {9B924EC5-BF13-3A98-8AC0-80877995D403}  
 System.Runtime.Remoting.Metadata.SoapAttribute  
 {9BF86F6E-B0E1-348B-9627-6970672EB3D3}  
 System.Runtime.Serialization.OnSerializingAttribute  
 {9C125A6F-EAE2-3FC1-97A1-C0DCEAB0B5DF} System.StackOverflowException  
 {9C67F424-22DC-3D05-AB36-17EAF95881F2}  
 System.Runtime.Remoting.Metadata.SoapTypeAttribute  
 {9D309F77-4655-372E-84B0-B0FB4030F3B8}  
 System.Runtime.InteropServices.SetWin32ContextInIDispatchAttribute  
 {9DA2F8B8-59F0-3852-B509-0663E3BF643B} System.MulticastNotSupportedException  
 {9E28EF95-9C6F-3A00-B525-36A76178CC9C} System.Text.ASCIIEncoding  
 {9E31421C-2F15-4F35-AD20-66FB9D4CD428}  
 System.EnterpriseServices.RegistrationHelperTx  
 {9EA60ECA-3DCD-340F-8E95-67845D185999} System.Security.Cryptography.CryptoConfig  
 {A0E2E749-63CE-3651-8F4F-F5F996344C32}  
 System.Security.Cryptography.RSAOAEPKeyExchangeFormatter  
 {A0F5F5DC-337B-38D7-B1A3-FB1B95666BBF} System.Text.UnicodeEncoding  
 {A164C0BF-67AE-3C7E-BC05-BFE24A8CDB62} System.IO.IOException  
 {A1C0A095-DF97-3441-BFC1-C9F194E494DB} System.Exception  
 {A36738B5-FA8F-3316-A929-68099A32B43B} System.PlatformNotSupportedException  
 {A36E4EAF-EA3F-30A6-906D-374BBF7903B1} System.Runtime.Remoting.Contexts.Context  
 {A3A1F076-1FA7-3A26-886D-8841CB45382F}  
 System.Runtime.CompilerServices.CallConvCdecl  
 {A5448B7A-AA07-3C56-B42B-7D881FA10934} System.Security.Policy.ApplicationTrust  
 {A6673C32-3943-3BBB-B476-C09A0EC0BCD6} System.Security.Cryptography.SHA512Managed  
 {A7136BDF-B141-3913-9D1C-9BC5AFF21470}  
 System.Runtime.Remoting.Metadata.W3cXsd2001.SoapYearMonth  
 {A7248EC6-A8A5-3D07-890E-6107F8C247E5}  
 System.Runtime.InteropServices.InvalidComObjectException  
 {A7EDDCB5-6043-3988-921C-25E3DEE6322B} System.Security.Cryptography.HMACMD5  
 {A8D058C4-D923-3859-9490-D3888FC90439}  
 System.Runtime.Serialization.Formatters.SoapFault  
 {A8F03BE3-EDB7-4972-821F-AF6F8EA34884} WmiSecurityHelper Class

## SOFTWARE OUTPUT

{A8F9F740-70C9-30A7-937C-59785A9BB5A4} System.IO.DriveNotFoundException  
 {AA544D41-28CB-11D3-BD22-0000F80849BD} SymBinder  
 {AAD4BDD3-81AA-3ABC-B53B-D904D25BC01E} System.Data.MisalignedException  
 {AB558A90-77EC-3C9A-A7E3-7B2260890A84}  
 System.EnterpriseServices.CompensatingResourceManager.Compensator  
 {AD326409-BF80-3E0C-BA6F-EE2C33B675A5} System.EntryPointNotFoundException  
 {AD664904-FE8A-3217-BBF5-E6AB1D998F5F}  
 System.Security.Permissions.HostProtectionAttribute  
 {AE53ED01-CAB4-39CE-854A-8BF544EEEC35} System.Security.Cryptography.HMACSHA384  
 {AF60343F-6C7B-3761-839F-0C44E3CA06DA} System.Security.Cryptography.CspParameters  
 {AF8C5F8A-9999-3E92-BB41-C5F4955174CD} System.IO.FileLoadException  
 {AFAEF10F-1BC4-351F-886A-878A265C1862} System.Security.Policy.TrustManagerContext  
 {AFC681CF-E82F-361A-8280-CF4E1F844C3E}  
 System.Runtime.InteropServices.ExternalException  
 {AFEF65AD-4577-447A-A148-83ACADD3D4B9} System.Data.SqlClient.SqlClient.SQLDebugging  
 {B0F64827-79BB-3163-B1AB-A2EA0E1FDA23}  
 System.EnterpriseServices.Internal.ComSoapPublishError  
 {B406AC70-4D7E-3D24-B241-AEAEAC343BD9} System.MTAThreadAttribute  
 {B54E38F8-17FF-3D0A-9FF3-5E662DE2055F}  
 System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNotation  
 {B6EB52D5-BB1C-3380-8BCA-345FF43F4B04}  
 System.Security.Cryptography.DESCryptoServiceProvider  
 {B81CB5ED-E654-399F-9698-C83C50665786}  
 System.Runtime.InteropServices.OptionalAttribute  
 {BC5062B6-79E8-3F19-A87E-F9DAF826960C}  
 System.Runtime.Remoting.Services.EnterpriseServicesHelper  
 {BCB67D4D-2096-36BE-974C-A003FC95041B}  
 System.Runtime.CompilerServices.CallConvStdcall  
 {BDA7BEE5-85F1-3B66-B610-DDF1D5898006} System.FieldAccessException  
 {C016A313-9606-36D3-A823-33EBF5006189} System.IO.PathTooLongException  
 {C03880A5-0B5E-39AD-954A-CE0DCBD5EF7D} System.AppDomainManager  
 {C1ABB475-F198-39D5-BF8D-330BC7189661}  
 System.Security.Cryptography.FromBase64Transform  
 {C30ABD41-7B5A-3D10-A6EF-56862E2979B6}  
 System.Runtime.Remoting.Messaging.OneWayAttribute  
 {C41D0B30-A518-3093-A18F-364AF9E71EB7}  
 System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNegativeInteger  
 {C41FA05C-8A7A-3157-8166-4104BB4925BA}  
 System.Security.Cryptography.CryptographicUnexpectedOperationException  
 {C437AB2E-865B-321D-BA15-0C8EC4CA119B}  
 System.Runtime.CompilerServices.NativeCppClassAttribute  
 {C498F2D9-A77C-3D4B-A1A5-12CC7B99115D}  
 System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNmtoken  
 {C76B435D-86C2-30FD-9329-E2603246095C}  
 System.Runtime.Remoting.Metadata.SoapParameterAttribute  
 {C9F0A842-3CE1-338F-A1D4-6D7BB397BDAA}  
 System.Runtime.Remoting.Metadata.W3cXsd2001.SoapDay  
 {C9F61CBD-287F-3D24-9FEB-2C3F347CF570} System.RankException

## SOFTWARE OUTPUT

```

{CA35CB3D-0357-11D3-8729-00C04F79ED0D} Microsoft.IE.Manager
{CA805B13-468C-3A22-BF9A-818E97EFA6B7}
System.Runtime.InteropServices.SEHException
{CAA817CC-0C04-4D22-A05C-2B7E162F4E8F}
System.EnterpriseServices.Internal.SoapServerVRoot
{CAEC7D4F-0B02-3579-943F-821738EE78CC}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapMonth
{CBEEA915-4D2C-3F77-98E8-A258B0FD3CEF} System.ContextMarshalException
{CC20C6DF-A054-3F09-A5F5-A3B5A25F4CE6} System.DuplicateWaitObjectException
{CC77F5F3-222D-3586-88C3-410477A3B65D} System.NonSerializedAttribute
{CCF306AE-33BD-3003-9CCE-DAF5BEFEF611} System.OutOfMemoryException
{CDC70043-D56B-3799-B7BD-6113BBCA160A} System.MissingMemberException
{C DFA7117-B2A4-3A3F-B393-BC19D44F9749}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapAnyUri
{CF8F7FCF-94FE-3516-90E9-C103156DD2D5}
System.Runtime.Serialization.Formatter.InternalRM
{D049DC2B-82C3-3350-A1CC-BF69FEE3825E}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapTime
{D13B741D-051F-322F-93AA-1367A3C8Aafb}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapNcName
{D23D2F41-1D69-3E03-A275-32AE381223AC}
System.Runtime.Serialization.FormatterConverter
{D2548BF2-801A-36AF-8800-1F11FBF54361}
System.Security.Cryptography.MD5CryptoServiceProvider
{D2EAA715-DAC7-4771-AF5C-931611A1853C} WmiSinkDemultiplexor Class
{D41969A6-C394-34B9-BD24-DD408F39F261}
System.Resources.MissingSatelliteAssemblyException
{D5CB383D-99F4-3C7E-A9C3-85B53661448F}
System.Reflection.CustomAttributeFormatException
{D6D2034D-5F67-30D7-9CC5-452F2C46694F} System.TypeUnloadedException
{D74D613D-F27F-311B-A9A3-27EBC63A1A5D} System.Threading.Mutex
{D8013EEF-730B-45E2-BA24-874B7242C425} System.EnterpriseServices.Internal.Publish
{D8013EF1-730B-45E2-BA24-874B7242C425}
System.EnterpriseServices.Internal.IISVirtualRoot
{D8013FF1-730B-45E2-BA24-874B7242C425}
System.EnterpriseServices.Internal.GenerateMetadata
{D8A4F3EB-E7EC-3620-831A-B052A67C9944}
System.Runtime.Remoting.Metadata.W3cXsd2001.SoapQName
{D9035152-6B1F-33E3-86F4-411CD21CDE0E}
System.Security.Cryptography.RSACryptoServiceProvider
{DA317BE2-1A0D-37B3-83F2-A0F32787FC67}
System.Reflection.TargetParameterCountException
{DAA132BF-1170-3D8B-A0EF-E2F55A68A91D}
System.Security.Cryptography.TripleDESCryptoServiceProvider
{DAFB2462-2A5B-3818-B17E-602984FE1BB0} System.NotSupportedException
{DB13821E-9835-3958-8539-1E021399AB6C} System.Runtime.Remoting.ServerException
{DC5DA001-7CD4-11D2-8ED9-D8C857F98FE3} Cor Remote Loader, CorLoad, CorLoad 1
{DD5856E5-8151-3334-B8E9-07CB152B20A4}

```

## SOFTWARE OUTPUT

System.Runtime.Remoting.Channels.ClientChannelSinkStack  
 {DE47D9CF-0107-3D66-93E9-A8ACB06B4583}

System.Runtime.Remoting.Metadata.W3cXsd2001.SoapDuration  
 {DFD888A7-A6B0-3B1B-985E-4CDAB0E4C17D}

System.Diagnostics.SymbolStore.SymLanguageVendor  
 {E38DA416-8050-3786-8201-46F187C15213} System.Security.XmlSyntaxException  
 {E724B749-18D6-36AB-9F6D-09C36D9C6016} System.Text.StringBuilder  
 {E772BBE6-CB52-3C19-876A-D1BFA2305F4E}

System.Runtime.Serialization.FormatterServices.SoapMessage  
 {E786FB32-B659-3D96-94C4-E1A9FC037868} System.ExecutionEngineException  
 {E7D574D5-2E51-3400-9FB6-A058F2D5B8AB}

System.EnterpriseServices.Internal.ClientRemotingConfig  
 {E822F35C-DDC2-3FB2-9768-A2AEBCE7C40}

System.Runtime.Remoting.Services.TrackingServices  
 {E9148312-A9BF-3A45-BBCA-350967FD78F5} System.BadImageFormatException  
 {E947A0B0-D47F-3AA3-9B77-4624E0F3ACA4}

System.Runtime.CompilerServices.IDispatchConstantAttribute  
 {EAA78D4A-20A3-3FDE-AB72-D3D55E3AEFE6} System.TimeoutException  
 {EBAA029C-01C0-32B6-AAE6-FE21ADFC3E5D} System.Security.VerificationException  
 {EC3DAC94-DF80-3017-B381-B13DCED6C4D8} System.Globalization.ThaiBuddhistCalendar  
 {ECABAFD1-7F19-11D2-978E-0000F8757E2A}

System.EnterpriseServices.Internal.ClrObjectFactory  
 {ECC82A10-B731-3A01-8A17-AC0DDD7666CF} System.Security.HostProtectionException  
 {ED0BC45C-2438-31A9-BBB6-E2A3B5916419}

System.Runtime.CompilerServices.CallConvFastcall  
 {EE24A2C3-3AA2-33DA-8731-A4FCC1105813} System.Security.Policy.GacInstalled  
 {EE832CE3-06CA-33EF-8F01-61C7C218BD7E} System.Globalization.HijriCalendar  
 {EE96F4E1-377E-315C-AEF5-874DC8C7A2AA}

System.Security.Cryptography.RSAPKCS1KeyExchangeDeformatter  
 {EEF05C76-5C98-3685-A69C-6E1A26A7F846} System.Security.SecurityException  
 {EF24F689-14F8-4D92-B4AF-D7B1F0E70FD4}

System.EnterpriseServices.Internal.AppDomainHelper  
 {F00CA7A7-4B8D-3F2F-A5F2-CE4A4478B39C}

System.Runtime.Remoting.Metadata.W3cXsd2001.SoapEntity  
 {F12FDE6A-9394-3C32-8E4D-F3D470947284} System.Reflection.AssemblyName  
 {F1C3BF79-C3E4-11D3-88E7-00902754C43A}

System.Runtime.InteropServices.TypeLibConverter  
 {F1EBA909-6621-346D-9CE2-39F266C9D011}

System.Runtime.InteropServices.ComImportAttribute  
 {F59D514C-F200-319F-BF3F-9E4E23B2848C}

System.Runtime.Remoting.Metadata.W3cXsd2001.SoapBase64Binary  
 {F5E692D9-8A87-349D-9657-F96E5799D2F4} System.IO.MemoryStream  
 {F6914A11-D95D-324F-BA0F-39A374625290} System.DivideByZeroException  
 {F6B6768F-F99E-4152-8ED2-0412F78517FB}

System.EnterpriseServices.Internal.SoapServerTlb  
 {F8BE2AD5-4E99-3E00-B10E-7C54D31C1C1D} System.NotImplementedException  
 {FA0B54D5-F221-3648-A20C-F67A96F4A207}

System.Runtime.Remoting.Metadata.W3cXsd2001.SoapId

## SOFTWARE OUTPUT

```

{FC13A7D5-E2B3-37BA-B807-7FA6238284D5}
System.Security.Cryptography.SHA1CryptoServiceProvider
{FD8C8FCE-4F85-36B2-B8E8-F5A183654539}
System.Runtime.Remoting.Lifetime.ClientSponsor
{FDB2DC94-B5A0-3702-AE84-BBFA752ACB36}
System.Runtime.InteropServices.OutAttribute
{FDF9C30D-CCAB-3E2D-B584-9E24CE8038E3} System.Security.Cryptography.SHA1Managed
{FFC9F9AE-E87A-3252-8E25-B22423A40065} System.ThreadStaticAttribute
Tue Jul 14 04:54:11 2009 Z
{60254CA5-953B-11CF-8C96-00AA00B8708C} Shell Extension For Windows Script Host
{7E48C5CF-72F6-4C84-9F43-B04B87B31243} Scripting.Signer
{8066FB71-AFA1-343E-8070-44AB4F3F85C9}
{88E729D6-BDC1-11D1-BD2A-00C04FB9603F} Folder Redirection Editor
{90F1A06E-7712-4762-86B5-7A5EBA6BDB01} Microsoft Common Language Runtime Meta
Data V2
{90F1A06E-7712-4762-86B5-7A5EBA6BDB02} Microsoft Common Language Runtime Meta
Data V2
{92BDB7E4-F28B-46A0-B551-45A52BDD5125} PSFactoryBuffer
{9C86F320-DEE3-4DD1-B972-A303F26B061E} PSFactoryBuffer
{B81FF171-20F3-11d2-8DCC-00A0C9B00525} Type name parser and builder
{C40D66A0-E90C-46C6-AA3B-473E38C72BF2} Folder Redirection Editor
{C89AC250-E18A-4FC7-ABD5-B8897B6A78A5}
System.EnterpriseServices.RegistrationHelperTx
Tue Jul 14 04:54:10 2009 Z
{0c9ac398-8c78-4b4b-b8c6-675ed1b734a1} IP Route Helper Class
{0cdb500e-123f-4e98-b446-0f3eae3c7ebc} NetBt Helper Class
{0f3ed1f2-afdd-4b0c-b6d9-229c1bc58a08} IP Path Helper Class
{1b9f2bf2-27f5-4dec-a175-3cf7bb8cfd3e} IP Address Helper Class
{1e887b90-7201-431d-820e-36aa566e52f4} Tcp Window Scaling Helper Class
{1e94e93c-852d-47fb-9197-7edeb41101b0} IPHTTPS Helper Class
{25983561-9D65-49CE-B335-40630D901227} Microsoft IMAPI v2, Raw CD Image Creator
{27354124-7F64-5B0F-8F00-5D77AFBE261E} Microsoft IMAPI v2, Stream interleave
utility
{27354125-7F64-5B0F-8F00-5D77AFBE261E} Microsoft IMAPI v2, Stream concatenation
utility
{27354126-7F64-5B0F-8F00-5D77AFBE261E} Microsoft IMAPI v2, PRNG based stream
{27354127-7F64-5B0F-8F00-5D77AFBE261E} Microsoft IMAPI v2, Zero Stream
{27354128-7F64-5B0F-8F00-5D77AFBE261E} Microsoft IMAPI v2, RAW Disc-At-Once CD
Writer
{27354129-7F64-5B0F-8F00-5D77AFBE261E} Microsoft IMAPI v2, Audio CD Writer
{2735412A-7F64-5B0F-8F00-5D77AFBE261E} Microsoft IMAPI v2, Standard Data Writer
{2735412B-7F64-5B0F-8F00-5D77AFBE261E} Microsoft IMAPI v2, Media Erase
{2735412C-7F64-5B0F-8F00-5D77AFBE261E} Microsoft IMAPI v2, Write Engine
{2735412D-7F64-5B0F-8F00-5D77AFBE261E} Microsoft IMAPI v2, CD DVD Device Object
{2735412E-7F64-5B0F-8F00-5D77AFBE261E} Microsoft IMAPI v2, Disc Master
{27354130-7F64-5B0F-8F00-5D77AFBE261E} PSFactoryBuffer
{286AA738-2928-49af-A410-4118F5C31626} Dot3 Helper Class
{2959380c-1567-40ec-80b0-05907ad6f9de} IP Neighbor Helper Class

```

## SOFTWARE OUTPUT

```

{2C941FC5-975B-59BE-A960-9A2A262853A5} FileSystemImage Class
{2C941FCE-975B-59BE-A960-9A2A262853A5} BootOptions Class
{2C941FD4-975B-59BE-A960-9A2A262853A5} PSFactoryBuffer
{30655864-f8cd-45f9-b7d6-6721acb69c5e} Network Connection Helper Class
{4FDBC3E5-7121-4487-AB95-B58EC04648DB} Extensible Media Manager Helper Class
{520CCA61-51A5-11D3-9144-00104BA11C5E} Microsoft IMAPI Disc Recorder
{520CCA63-51A5-11D3-9144-00104BA11C5E} Microsoft IMAPI Disc Master
{6D54E523-3B26-41CB-9478-BAECBC255189} SPPCCHandler Class
{73257e95-0378-49d6-a954-44aabc841eab} Address Acquisition Helper Class
{862321c3-70b2-4ee2-8231-87ec05819d98} Transport Connection Helper Class
{8A03567A-63CB-4BA8-BAF6-52119816D1EF} Microsoft IMAPI Disc Recorder Enumerator
{B0DDD260-9E44-4bf2-8602-6D9CE1D0B94F} UCM Helper Class
{b11d16d0-e195-4ca6-bbd5-1254ec098953} 6To4 Helper Class
{bd69ecaa-ae5c-40d0-b968-7848f3778f56} DHCP Module Helper Class
{CEEE3B62-8F56-4056-869B-EF16917E3EFC} Microsoft IMAPI v2, .ISO Image Manager
utility
{EFB92EFB-9236-4bd7-B60D-51D1C7D1C87A} Framing Layer Helper Class
{FE217CB2-0B2C-48c9-90CA-8D8BCA79248D} Teredo Helper Class
Tue Jul 14 04:54:09 2009 Z
{00BC7EAE-28D5-4310-BE9F-11526A7FA37F} ModemActivation Class
{0A14D3FF-EC53-450f-AA30-FFBC55BE26A2} TokenActivation Class
{179CC917-3A82-40E7-9F8C-2FC8A3D2212B} SPPLUAObject Class
{32be5ed2-5c86-480f-a914-0ff8885a1b3f} RDPViewer Class
{6ACB028E-48C0-4A44-964C-E14567C578BA} SppWmiProvider
{7DA49535-DB7D-47d5-9552-6DAEFA831E64}
{8A99553A-7971-4445-93B5-AAA43D1433C5} OfflineActivation Class
{91ECFDB4-2606-43E4-8F86-E25B0CB01F1E} ElevationConfig Class
{9B78F0E6-3E05-4A5B-B2E8-E743A8956B65} RDPSession Class
{A49211A1-022F-43D7-BC55-D787C66ACF8E} LicensingPackage Class
{A4DDCA2B-E73C-40C5-83B1-9F40269D0B0D} OnlineActivation Class
{A6C13C9D-54E1-44FC-82F0-DBE2C843E51A} SPPUIObject Class
{AA04CA0B-7597-4F3E-99A8-36712D13D676} LicensingStateTools Class
{b3179149-2b99-48b2-b44b-11aa2034c1a3} CCNGProvider
{b6dc98b1-0bec-45e1-b2e4-3a2d943f0be4} CDPAPIProvider
{CB6E2B90-25FA-4F08-B46C-696F5A2B6CA5} SppWmiTokenActivationSigner
{CD8534F7-B1CE-4A6B-B7CD-AA4AE578A20A} LicensingStatusData Class
{e5899c7c-0fc7-499e-a262-174fd692dc9f} CCAPIProvider
{F87B28F1-DA9A-4F35-8EC0-800EFCF26B83} SPPUIObjectInteractive Class
{f91b9abc-985b-4c04-b5e7-9c7099fc2cda} CADProvider
{ff8a71c2-7eb8-418b-950d-3b49f43f024f} CWinCredProvider
Tue Jul 14 04:54:08 2009 Z
{6377013E-2C35-40F3-B8E1-1AB47D12982B} WABSyncProvider
{6E582707-CCAF-4333-A9B9-3B4F75C362E0} DeviceOwnershipControl Class
{8373ce97-72b7-4fb2-b5e8-b38aa083d734} WinSync Anchor Provider Wrapper
{896C2B1D-3586-4FA5-B419-41F4A6D38CF1} SyncInfrastructureControl Class
{a10dfc9e-ff12-4e7f-bc74-8fe9053920f0} WinSync Full Enumeration Provider Wrapper
{A38F4597-F640-4189-982F-132ECF8202FA} WPDSyncProvider Class
{a4a8d991-cc85-493e-ae66-9a847402dad9} FD Device Pairing Configuration

```

## SOFTWARE OUTPUT

{a4a8d991-cc85-493e-ae66-9a847402dada} Device Pairing Config Proxy  
 {c27f6b1d-fe0b-45e4-9257-38799fa69bc8} UsbCeip  
 {C947D50F-378E-4FF6-8835-FCB50305244D} SyncInfrastructure Class  
 {F82B4EF1-93A9-4DDE-8015-F7950A1A6E31} Sync Registration  
 {F9EBBF2D-0C5D-4BF1-AE24-A30F7796D178} PSFactoryBuffer  
 {FF3AE31D-55B0-4945-BDE9-622ABB334C1A} WABSyncConfigUI

Tue Jul 14 04:54:07 2009 Z

{25B25D91-69A2-47fa-A375-FDC98189A06F}  
 {28803F59-3A75-4058-995F-4EE5503B023C} Bluetooth Devices  
 {347CBD95-DD80-4144-81AF-AE803E633A00} PSFactoryBuffer  
 {42060D27-CA53-41f5-96E4-B1E8169308A6} ReliabilityAnalysisCustomHandler  
 {5F02227D-BF38-48BE-B01A-A47D3006DFA2} WPDDispatchFactory Class  
 {8FD8B88D-30E1-4F25-AC2B-553D3D65F0EA} DXP  
 {AEE2420F-D50E-405C-8784-363C582BF45A} DevicePairingFolder Initialization  
 {b8f87e75-d1d5-446b-931c-3f61b97bca7a}  
 {D0520B5D-1B5F-4ECF-A940-6E57476AE4B0}  
 {D7C3453E-1F1C-48CD-AFE6-CFF2A937D337}  
 {DC79A5C8-CCAD-4698-9034-C4C8068011C5} PSFactoryBuffer  
 {E2E5A310-ECED-444F-81D7-ACCA6AC8A1A8} Win32\_TpmProvider Class  
 {F022A390-2F1E-44d2-AA0A-0FEB28AE6517} DXP  
 {F1EFACAA-08A1-461B-9D28-7AA8947889A0}

Tue Jul 14 04:54:06 2009 Z

{022B358F-06B8-4E0D-ADD9-655A8F1E9EDD}  
 {04DA8451-7F63-4870-A4D7-F55BE66BFDFB}  
 {05C9DA2B-6DFF-42C7-81CC-706DAE08BC7A}  
 {095D3BE1-A874-46A5-B989-AE43E3427E3C}  
 {0D722F1A-9FCF-4E62-96D8-6DF8F01A26AA} SpShortcut Class  
 {0E1EEFB2-E336-481C-B178-36261EC5A843}  
 {0F0549A6-C2E0-442A-85D7-20E3DB9B6A1F}  
 {0F92030A-CBFD-4AB8-A164-FF5985547FF6} SpTextSelectionInformation Class  
 {10A2BDBC-7130-420C-9320-A92CC1919206}  
 {12D73610-A1C9-11D3-BC90-00C04F72DF9F} SpITNProcessor Class  
 {136E0057-D7ED-4B85-9F62-1318CFE1573B}  
 {1A3ED173-B201-4470-9FC6-EC46CF8D56F1}  
 {1B2AFB92-0B5E-4A30-B5CC-353DB4F9E150} SpSapiServer Class  
 {1B57B2A1-E763-4676-9064-297F1B413632} SpMMAudioInLegacy Class  
 {1C0D39B2-C788-40D2-B062-FDF8293D7BC6}  
 {1D49F57D-47D2-4AEE-A69B-593EC558773F}  
 {1E69A8EB-0B11-40C3-AC27-906ED77CD946}  
 {212ADF89-1F86-49D0-914A-DF6C5613C81E}  
 {2652B813-2260-4EF3-A311-74A7AC6513D7}  
 {2C9F6BEB-C5B0-42B6-A5EE-84C24DC0D8EF}  
 {2CB6CDA4-1C14-4392-A8EC-81EEF1F2E079}  
 {2CB861BB-B1B4-4E14-A1A7-D3FB30C3F5CF}  
 {2D12DD17-6C4E-456E-A953-D210E3C64176} SpCommunicator Class  
 {333E6924-4353-4934-A7BE-5FB5BDDDB2D6}  
 {3BEE4890-4FE9-4A37-8C1E-5E7E12791C1F} SpSharedRecognizer Class  
 {3D0B8752-68F8-4F39-929D-DE20ED323F45}

## SOFTWARE OUTPUT

```

{3D5DF14F-649F-4CBC-853D-F18FEDE9CF5D}
{3FAA93F3-79FB-4319-8387-B8FFE074FBDA}
{41B89B6B-9399-11D2-9623-00C04F8EE628} SpInprocRecognizer Class
{42001A23-ED2A-4582-8BCC-6320C543E102}
{4495524E-2E54-472D-86D7-D671CA588F01}
{45EACA36-DBE9-4E4A-A26D-5C201902346D}
{47206204-5ECA-11D2-960F-00C04F8EE628} SpSharedRecoContext Class
{483B0283-25DB-4C92-9C15-A65925CB95CE}
{49C69FAB-ED5E-4D48-9A65-E4816E5FE642}
{52BE2F87-1638-408A-9A98-74239B0B7DB5}
{530CC6A4-357F-49E2-AB11-3C481DBEDE31}
{53DA1CBB-0F45-46A4-AA6E-47CAAD84C921}
{55DFB4F7-4175-4B3B-B247-D9B399ADB119} MSTTS Frontend Class (ENU)
{5F104B61-7998-4049-A7BB-C99EFB6B4A4E}
{610133F4-ED38-42E7-9C18-EB2A8F76B99A}
{61A48126-EF74-4D4A-9DDA-43FD542CAD1E}
{61DBD86A-8D1A-4EB0-907C-E4C1BBC8F09A}
{65170AE4-0AD2-4FA5-B3BA-7CD73E2DA825}
{68DC71DC-2327-4040-8F03-50D6A9805049}
{697E2FF0-7FA8-49F1-BB4A-E1D115AA2BBB}
{69ED626B-904D-4DEF-B919-9EF7E4E339DD}
{6C53A912-47C6-4959-B342-DF6C9DA9D494}
{70878DCD-56F6-4681-BC52-BC7F58EDF723}
{712720F4-F4FF-46CF-B6EC-2CC24FC873A5}
{73AD6842-ACE0-45E8-A4DD-8795881A2C2A} SpInProcRecoContext Class
{773229CD-D53C-4211-ACD8-8F2C7BF2AE7C}
{776266FF-0DC5-4F45-BADA-39A7586FACE2}
{777B6BBD-2FF2-11D3-88FE-00C04F8EF9B5} SpPhraseBuilder Class
{7AE7416D-AD97-4A4B-B5AC-B3CA7865AFBE}
{7E352021-69D6-4553-86AC-430B0D8FF913}
{7EFD3C7E-9E4B-4A93-9503-DECD74C0AC6D}
{81442F68-A942-457E-9AF0-C6977E244A7C}
{818C68B0-D4C9-475C-B2CF-AF4242F27C8D}
{86781CF9-799C-4CFF-9AA5-43F4C23FF866}
{874131cb-4ecc-443b-8948-746b89595d20} WMSpeech Decoder DMO
{87824713-C8B0-4379-8556-1689764E4237}
{89EA5B5A-D01C-4560-A874-9FC92AFB0EFA}
{89F38560-A0AE-4D8C-9E8F-83D4DB8A9F85}
{8A899610-150A-40DB-B57A-940EDB3203CE}
{8B3302D7-95F6-4BC5-A06A-0D6DEF15DB69}
{8E67B6EF-205D-490F-A004-7B04F8F65B62}
{92F2118A-E813-4A4D-9DE2-F96A9DC02C53}
{9CDAEA40-A7D3-4cc5-AED0-B5E35AD0F169} SpW3CSemanticInterpretation Class
{9D0EAB8C-8EF4-4020-B867-2B1E04E4B8E5}
{9DAA54E8-CD95-4107-8E7F-BA3F24732D95}
{9FE6E853-B35F-4FE4-B006-33148455093E}
{A0A5A274-A190-4A81-997B-9593D6F6D462}
{A25A5CCD-80F4-4E02-AADD-7F39CC55E737}

```



## SOFTWARE OUTPUT

```

{A9C6B8DD-3CBB-44CB-AA44-4B1C0DBB404D}
{B1E29D59-A675-11D2-8302-00C04F8EE6C0} SpGrammarCompiler Class
{B675B948-FBA8-46A4-A4C7-D4291785127B}
{C23FC28D-C55F-4720-8B32-91F73C2BD5D1} SpPhraseInfoBuilder Class
{C28DA8E5-39C2-4F62-82FA-C61D39A196DF}
{C4BF21DA-F1E5-4C7F-A611-2698645B19EF}
{C700F6EF-A80F-4B24-922A-32308B6FF0C3}
{CA0AC604-8EF2-448A-AE97-62A2C2CC3C46} SpDMOAudioIn Class
{CF3D2E50-53F2-11D2-960C-00C04F8EE628} SpMMAudioIn Class
{D0458F37-2228-4FC7-9E66-34133DF4C929}
{D2C13906-51EF-454e-BC67-A52475FF074C} SpW3CGrammarCompiler Class
{D36D2090-4DF3-4bd4-A22F-0D91975F7964} SpMSSemanticInterpretation Class
{D385FDAD-D394-4812-9CEC-C6575C0B2B38}
{D6AD10F3-70AB-41E1-96B3-4C36E35D333C} SpRecoMaster Class
{D9581C03-9766-45A6-B970-1EABBE985986}
{DA93E903-C843-11D2-A084-00C04F8EF9B5} SpGramCompBackEnd Class
{DC4701DE-1014-44CC-85A6-253F2B30FB9E}
{DC626A64-D684-4627-83CB-44420ABDBD1A} SpSharedRecoInst Class
{E06A0DDD-E81A-4E93-8A8D-F386C3A1B670}
{E1E0A883-AB68-4C6C-9C8C-808AF2BA4CBA}
{E1E8F15E-8BEC-45DF-83BF-50FF84D0CAB5}
{E58FA315-E206-4CA4-81CE-F34E18E672C9}
{E5B2CB7A-FD35-4D4B-A147-176FEB42244B}
{E7B6AEE0-84AE-46CE-B450-DEBF58C90889}
{EB6C9433-4AAB-4B71-8B18-8F7A3812E43A}
{EE38A9FC-437F-4D03-A593-BB92AF0D153C}
{F3AEB884-58C8-40CF-AED3-E7EEFFFAA04A}
{F3D3F924-11FC-11D3-BB97-00C04F8EE6C0} SpCFGEngine Class
{F51C7B23-6566-424C-94CF-2C4F83EE96FF} MS TTSEngine Class
{F66A6818-F490-431B-8CA4-4CFDA287327B} MSTTS LTS Class
{F7A465EE-13FB-409A-B878-195B420433AF}
{F7B02D8A-65DB-41CB-894D-5BBBF96C1B42}
{FBA89535-BFAB-4EF7-804C-109186BF507B}
{FD339D76-EA3E-435F-AC29-3FFCE55EB35B}
{FD51544B-8050-4C68-ABAE-3E1F7A8C01D3}
Tue Jul 14 04:54:05 2009 Z
{FCDECE00-A39D-11D0-ABE7-00AA0064D470} ScriptoSys Class
Tue Jul 14 04:54:02 2009 Z
{0655E396-25D0-11D3-9C26-00C04F8EF87C} SpLexicon Class
{25642426-028D-4474-977B-111BB114FE3E} PSFactoryBuffer
{3918D75F-0ACB-41F2-B733-92AA15BCECF6} SpObjectTokenEnum Class
{455F24E9-7396-4A16-9715-7C0FDBE3EFE3} SpNullPhoneConverter Class
{4C6F940C-3CFE-11D2-9EE7-00C04F797396} SpTaskManager Class
{4F414126-DFE3-4629-99EE-797978317EAD} SpPhoneticAlphabetConverter Class
{5440837F-4BFF-4AE5-A1B1-7722ECC6332A} AccStore Class
{5FB7EF7D-DFF4-468a-B6B7-2FCBD188F994} SpMemoryStream Class
{6089A37E-EB8A-482D-BD6F-F9F46904D16D} AccServerDocMgr Class
{6572EE16-5FE5-4331-BB6D-76A49C56E423} AccDictionary Class

```

## SOFTWARE OUTPUT

```

{7013943A-E2EC-11D2-A086-00C04F8EF9B5} SpStreamFormatConverter Class
{715D9C59-4442-11D2-9605-00C04F8EE628} SpStream Class
{8DBEF13F-1948-4AA8-8CF0-048EEBED95D8} SpCustomStream Class
{90903716-2F42-11D3-9C26-00C04F8EF87C} SpCompressedLexicon Class
{9185F743-1143-4C28-86B5-BFF14F20E5C8} SpPhoneConverter Class
{947812B3-2AE1-4644-BA86-9E90DED7EC91} SpFileStream Class
{96749373-3391-11D2-9EE3-00C04F797396} SpResourceManager Class
{96749377-3391-11D2-9EE3-00C04F797396} SpVoice Class
{9EF96870-E160-4792-820D-48CF0649E4EC} SpAudioFormat Class
{A8C680EB-3D32-11D2-9EE7-00C04F797396} SpMMAudioOut Class
{A910187F-0C7A-45AC-92CC-59EDAFB77B53} SpObjectTokenCategory Class
{AB1890A0-E91F-11D2-BB91-00C04F8EE6C0} SpMMAudioEnum Class
{BF426F7E-7A5E-44D6-830C-A390EA9462A3} DocWrap Class
{C02F29F0-DFCA-4DC1-8B80-ED3216E1B5E0} SpTtsFormatConverter Class
{C79A574C-63BE-44b9-801F-283F87F898BE} SpWaveFormatEx Class
{C9E37C15-DF92-4727-85D6-72E5EEB6995A} SpUncompressedLexicon Class
{D9F6EE60-58C9-458B-88E1-2F908FD7F87C} SpDataKey Class
{E2AE5372-5D40-11D2-960E-00C04F8EE628} SpNotifyTranslator Class
{EF411752-3736-4CB4-9C8C-8EF4CCB58EFE} SpObjectToken Class
{FC48CC30-4F3E-4fa1-803B-AD0E196A83B1} AccClientDocMgr Class
Tue Jul 14 04:54:01 2009 Z
{1F5EEC01-1214-4D94-80C5-4BDCD2014DDD}
{434A6274-C539-4E99-88FC-44206D942775} AccessibilityCplAdmin Class
{483afb5d-70df-4e16-abdc-a1de4d015a3e} AzPrincipalLocator Class
{5c2dc96f-8d51-434b-b33c-379bccae77c3} AzBizRuleContext Class
{93CB110F-9189-4349-BD9F-392D9A4D0096} Accessibility Control Panel
{b2bcff59-a757-4b0b-a1bc-ea69981da69e} AzAuthorizationStore Class
{D555645E-D4F8-4c29-A827-D93C859C4F2A} Ease of Access
{FA9342F0-B15B-473C-A746-14FCD4C4A6AA}
Tue Jul 14 04:54:00 2009 Z
{8cec58e7-07a1-11d9-b15e-000d56bfe6ee} AP Client HxHelpPane Class
Tue Jul 14 04:53:59 2009 Z
{31b7c920-2880-11d0-8d51-00a0c908dbf1} Korean_Default Word Breaker Resources
{369647e0-17b0-11ce-9950-00aa004bbb1f} Neutral Word Breaker
{37c84fa0-d3db-11d0-8d51-00a0c908dbf1} Korean_Default Stemmer Resources
{4662DAA5-D393-11D0-9A56-00C04FB68BF7}
{4662DAA6-D393-11D0-9A56-00C04FB68BF7}
{4662DAA7-D393-11D0-9A56-00C04FB68BF7}
{4662DAA8-D393-11D0-9A56-00C04FB68BF7}
{4662DAA9-D393-11D0-9A56-00C04FB68BF7}
{4662DAAA-D393-11D0-9A56-00C04FB68BF7}
{4662DAAB-D393-11D0-9A56-00C04FB68BF7}
{4662DAAC-D393-11D0-9A56-00C04FB68BF7}
{4662DAAD-D393-11D0-9A56-00C04FB68BF7}
{4662DAAE-D393-11D0-9A56-00C04FB68BF7}
{4662DAAF-D393-11D0-9A56-00C04FB68BF7}
{4662DAB0-D393-11D0-9A56-00C04FB68BF7}
{5D02926A-212E-11D0-9DF9-00A0C922E6EC} Microsoft InfoTech IStorage System

```

## SOFTWARE OUTPUT

{8cec58ae-07a1-11d9-b15e-000d56bfe6ee} AP Client HxHelpPaneServer Class  
 {8FA0D5A8-DEDF-11D0-9A61-00C04FB68BF7}  
 {9D148290-B9C8-11D0-A4CC-0000F80149F6} Microsoft InfoTech Protocol for IE 3.0  
 {9D148291-B9C8-11D0-A4CC-0000F80149F6} Microsoft InfoTech Protocols for IE 4.0  
 {cca22cf4-59fe-11d1-bbff-00c04fb97fda} Thai\_Default Word Breaker Resources  
 {cedc01c7-59fe-11d1-bbff-00c04fb97fda} Thai\_Default Stemmer Resources  
 {D54EEE56-AAAB-11D0-9E1D-00A0C922E6EC} Microsoft InfoTech IStorage for Win32

## Files

Tue Jul 14 04:53:58 2009 Z

{023A36FC-E9D5-419E-824A-CDC66A116E84} Windows Firewall with Advanced Security  
 {0E752416-F29E-4195-A9DD-7F0D4D5A9D71} Windows Firewall with Advanced Security  
 {12a66224-5e8a-4679-8941-0b9b960bf5ea} VistaWUWebControl Class  
 {12CE94A0-DEFB-11D2-B31D-00600893A857} Chinese\_Simplified Word Breaker Resources  
 {1CD0938D-1AC1-49DE-AA04-F2C92D4A02D1}  
 {2e2294a9-50d7-4fe7-a09f-e6492e185884} rtf persistent handler  
 {3a64898b-20a7-4384-894b-7273c3539f2f} MIME Filter PersistentHandler  
 {5645C8C1-E277-11CF-8FDA-00AA00A14F93}  
 {5645C8C2-E277-11CF-8FDA-00AA00A14F93} MIME Filter  
 {5645C8C4-E277-11CF-8FDA-00AA00A14F93}  
 {73FDCC80-AEA9-101A-98A7-00AA00374959} WordPad Document  
 {752438CB-E941-433F-BCB4-8B7D2329F0C8} FwCpl LUA  
 {954F1760-C1BC-11D0-9692-00A0C908146E} Chinese\_Traditional Word Breaker Resources  
 {A4B07E49-6567-4FB8-8D39-01920E3B2357} Virtual Factory for Windows Firewall Cpl  
 {ce8dbe60-d37a-4bdd-ab3a-399e69489182}  
 {DDECE4B2-979F-4CDB-9F58-B036FE5A510C} Firewall Control Panel  
 {e2403e98-663b-4df6-b234-687789db8560} RTF Filter  
 {E7E6A098-87CE-420D-91AE-413312AC8FA6} Windows Firewall Helper Class

Tue Jul 14 04:53:55 2009 Z

{011BE22D-E453-11D1-945A-00C04FB984F9} WSecEdit Security Manager Class  
 {116ABC1A-F7DB-45A7-ADDA-D5A57A08C6FF} Workspace Setup Input Page  
 {165D4642-1278-4486-A3FD-439F5888FCA3} Workspace Setup Message Page 2  
 {18b726bb-6fe6-4fb9-9276-ed57ce7c7cb2} KMRDPProtocolManager Class  
 {1B462D7B-72D8-4544-ACC1-D84E5B9A8A14} MsRdpSessionManager Class  
 {1B6FC61A-648A-4493-A303-A1A22B543F01} WSecEdit RSOP Security Settings Class  
 {1D428C79-6E2E-4351-A361-C0401A03A0BA} PSFactoryBuffer  
 {228D9A81-C302-11cf-9AA4-00AA004A5691} LDAP Provider Object  
 {228D9A82-C302-11cf-9AA4-00AA004A5691} LDAP Namespace Object  
 {22B6E688-B3A5-44FC-B0CE-69F20653CD61} Workspace Setup Finish Page  
 {241D7C96-F8BF-4F85-B01F-E2B043341A4B} Workspaces Center  
 {250e91a0-0367-11cf-abc4-02608c9e7553} WinNT Namespace Object  
 {274fae1f-3626-11d1-a3a4-00c04fb950dc} ADs LDAP NameTranslate Object  
 {286F484D-375E-4458-A272-B138E2F80A6A} DirectPlay8Peer Object  
 {2AABFCD0-1797-11D2-ABA2-00C04FB6C6FA} WSecEdit Security Configuration Class  
 {2BB8B28A-58DC-449C-A89B-DAEFD0A8933D}  
 {2dfb3a35-6071-11d1-8c13-00c04fd8d503} Microsoft Locality Extension  
 {2E8EA1E5-F406-46F5-AF10-661FD6539F28} WSecEdit Local Security Settings Class  
 {3B2B6775-70B6-45AF-8DEA-A209C69559F3} DirectPlay8LobbyClient Object  
 {3DECD5DD-A27B-48DC-8BAA-2682CFA265FF} Workspace Setup Message Page

## SOFTWARE OUTPUT

```

{4de7016c-5ef9-11d1-8c13-00c04fd8d503} Microsoft User Extension
{4F1DFCA6-3AAD-48E1-8406-4BC21A501D7C} Workspace Class
{50B6327F-AFD1-11d2-9CB9-0000F87A369E} AD System Info Object
{59CDB915-8232-46AD-B38B-497B8B0463AD} Workspace Setup Configure Page
{5ADF5BF6-E452-11D1-945A-00C04FB984F9} WSecEdit Security Configuration Class
{5C0786ED-1847-11D2-ABA2-00C04FB6C6FA} WSecEdit Security Manager Class
{5C0786EE-1847-11D2-ABA2-00C04FB6C6FA} WSecEdit Security Settings Class
{66182EC4-AFD1-11d2-9CB9-0000F87A369E} WinNT System Info Object
{667955AD-6B3B-43CA-B949-BC69B5BAFF7F} DirectPlay8LobbiedApplication Object
{6A5B0C7C-5CCB-4F10-A043-B8DE007E1952} MsRdpClientShell Class
{6D4A3650-628D-11D2-AE0F-006097B01411} DirectPlay8 Modem Provider Object
{743B5D60-628D-11D2-AE0F-006097B01411} DirectPlay8 Serial Provider Object
{743F1DC6-5ABA-429F-8BDF-C54D03253DC2} DirectPlay8Client Object
{7940ACF8-60BA-4213-A7C3-F3B400EE266D} Setup a Workspace Task Class
{803E14A0-B4FB-11D0-A0D0-00A0C90F574B} WSecEdit Extension Class
{8b20cd60-0f29-11cf-abc4-02608c9e7553} WinNT Provider Object
{934A9523-A3CA-4BC5-ADA0-D6D95D979421} DirectPlay8Address Object
{94a909a5-6f52-11d1-8c18-00c04fd8d503} Microsoft Group Extension
{984F9804-3314-4FA4-AC8C-E688D4133C51} Workspace Setup Confirm Settings Page
{9f37f39c-6f49-11d1-8c18-00c04fd8d503} Microsoft PrintQueue Extension
{B43A0C1E-B63F-4691-B68F-CD807A45DA01} MSTWebProxy Class
{BB0D7187-3C44-11D2-BB98-3078302C2030} CfgComp Class
{BBC035D1-E5A1-44F5-A166-E70DAED1CB02}
{CFF49D53-EE51-49F2-A807-7E3DF4EA36E3} WSecEdit Local Security Settings Class
{D5AB5662-131D-453D-88C8-9BBA87502ADE}
Microsoft.ManagementConsole.Advanced.FrameworkSnapInFactory
{DA825E1B-6830-43D7-835D-0B5AD82956A2} DirectPlay8Server Object
{dccc0bed-6066-11d1-8c13-00c04fd8d503} Microsoft Organization Extension
{E4C1D9A2-CBF7-48BD-9A69-34A55E0D8941} DirectPlay8 NAT Resolver Object
{EBFE7BA0-628D-11D2-AE0F-006097B01411} DirectPlay8 WSock TCPIP Provider Object
{EFEA49A2-DDA5-429D-8F42-B23B92C4C347} PSFactoryBuffer
{F0152790-D56E-4445-850E-4F3117DB740C} Remote Sessions CPL Extension
{F975AF2C-9A51-4AF0-91EA-06038698CE38} DirectPlay8 Diagnostics Object
{FC47060E-6153-4B34-B975-8E4121EB7F3C} DirectPlay8 Thread Pool Object
{fd8d3a5f-6066-11d1-8c13-00c04fd8d503} Microsoft OrganizationUnit Extension
{FE883157-CEBD-4570-B7A2-E4FE06ABE626} WSecEdit RSOP Security Settings Class
Tue Jul 14 04:53:54 2009 Z
{01FA60A0-BBFF-11D0-8825-00A0C903B83C} Encode CRL Distribution Points Class
{02E6EC4C-96E4-42E8-B533-336916A0087D} PSFactoryBuffer
{19A76FE0-7494-11D0-8816-00A0C903B83C} Encode String Array Class
{1CFC4CDA-1271-11D1-9BD4-00C04FB683FA} Encode Alternate Name Class
{301F77B0-A470-11D0-8821-00A0C903B83C} Encode Date Array Class
{3523c2fb-4031-44e4-9a3b-f1e94986ee7f} Microsoft RDP Client Control - version 3
{4E0680A0-A0A2-11D0-8821-00A0C903B83C} Encode Long Array Class
{4eb2f086-c818-447e-b32c-c51ce2b30d31} Microsoft RDP Client Control - version 6
{4eb89ff4-7f78-4a0f-8b8d-2bf02e94e4b2} Microsoft RDP Client Control
(redistributable) - version 6
{4EDCB26C-D24C-4e72-AF07-B576699AC0DE} Microsoft RDP Client Control

```

## SOFTWARE OUTPUT

```

(redistributable) - version 5
  {54CE37E0-9834-41ae-9896-4DAB69DC022B} Microsoft RDP Client Control
(redistributable) - version 5a
  {54d38bf7-b1ef-4479-9674-1bd6ea465258} Microsoft RDP Client Control - version 8
  {6A6F4B83-45C5-4ca9-BDD9-0D81C12295E4} Microsoft RDP Client Control
(redistributable) - version 4a
  {6AE29350-321B-42be-BBE5-12FB5270C0DE} Microsoft RDP Client Control - version 5
  {6D6B3CD8-1278-11D1-9BD4-00C04FB683FA} Encode Bit String Class
  {7390f3d8-0439-4c05-91e3-cf5cb290c3d0} Microsoft RDP Client Control
(redistributable) - version 7
  {7584c670-2274-4efb-b00b-d6aaba6d3850} Microsoft RDP Client Control
(redistributable) - version 4
  {7cacbd7b-0d99-468f-ac33-22e495c0afe5} Microsoft RDP Client Control - version 2
  {9059f30f-4eb1-4bd2-9fdc-36f43a218f4a} Microsoft RDP Client Control
(redistributable) - version 3
  {971127BB-259F-48c2-BD75-5F97A3331551} Microsoft RDP Client Control
(redistributable) - version 3a
  {A1230201-1439-4E62-A414-190D0AC3D40E} PSFactoryBuffer
  {A1230401-67a5-4df6-a730-dce8822c80c4}
  {a41a4187-5a86-4e26-b40a-856f9035d9cb} Microsoft Terminal Services Client Control
- version 1
  {a9d7038d-b5ed-472e-9c47-94bea90a5910} Microsoft RDP Client Control
(redistributable) - version 8
  {aac1009f-ab33-48f9-9a21-7f5b88426a2e} TSRDSettings Class
  {ace575fd-1fcf-4074-9401-ebab990fa9de} Microsoft RDP Client Control - version 4
  {d2ea46a7-c2bf-426b-af24-e19c44456399} Microsoft RDP Client Control - version 7
  {F9A874B6-F8A8-4D73-B5A8-AB610816828B} Terminal Services Connection Manager Class
Tue Jul 14 04:53:53 2009 Z
  {27016870-8E02-11D1-924E-00C04FBBBFB3} MS Remote
  {280A7B65-8F00-438F-989B-8EAF9E438A71}
  {3449A1C8-C56C-11D0-AD72-00C04FC29863} MSDataShape
  {34AB8E82-C27E-11D1-A6C0-00C04FB94F17}
  {53D6AB1D-2488-11D1-A28C-00C04FB94F17}
  {69A25C12-1811-11D2-A52B-0000F803A951}
  {69A25C14-1811-11D2-A52B-0000F803A951}
  {93F7AA8E-CF82-4CB7-9251-48BC637A43B8}
  {A1A6B99D-497F-11D1-9217-00C04FBBBFB3} Handler Class
  {E3E1D967-0829-48AC-B3AD-C5AE4CA171C4} SQLXMLX.1
Tue Jul 14 04:53:52 2009 Z
  {06210E88-01F5-11D1-B512-0080C781C384} PSFactoryBuffer
  {0C7FF16C-38E3-11d0-97AB-00C04FC2AD98} SQLOLEDB
  {0FB15084-AF41-11CE-BD2B-204C4F4F5020} PSFactoryBuffer
  {54AF9350-1923-11D3-9CA4-00C04F72C514} MDACVer.Version
  {9381D8F5-0288-11d0-9501-00AA00B911A5} RDS.Server.DataFactory
  {BD96C556-65A3-11D0-983A-00C04FC29E33} RDS.DataControl
  {BD96C556-65A3-11D0-983A-00C04FC29E36} RDS.DataSpace
  {C0932C62-38E5-11d0-97AB-00C04FC2AD98} SQLOLEDB Error Lookup
  {c8b522cb-5cf3-11ce-ade5-00aa0044773d} MSDASQL

```

## SOFTWARE OUTPUT

```

{c8b522cc-5cf3-11ce-ade5-00aa0044773d} MSDASQL ErrorLookup
{c8b522cd-5cf3-11ce-ade5-00aa0044773d} MSDASQL Enumerator
{DFA22B8E-E68D-11d0-97E4-00C04FC2AD98} SQLOLEDB Enumerator
{dfc8bdc0-e378-11d0-9b30-0080c7e9fe95} MSDAOSP
{ef636390-f343-11d0-9477-00c04fd36226} OLE DB Rowset Proxy
{ef636391-f343-11d0-9477-00c04fd36226} OLE DB Rowset Server
{ef636392-f343-11d0-9477-00c04fd36226} OLE DB Row Proxy
{ef636393-f343-11d0-9477-00c04fd36226} OLE DB Row Server
Tue Jul 14 04:53:51 2009 Z
{016fd94e-b02a-4ab8-94c6-149fdab56b8d} PSFactoryBuffer
{1d16438c-54dc-404f-83a9-c041e77a32dd} DTC Transaction Stats Control
{1f09b058-f3fd-4a9d-a8ba-a8a05f8fe283} DTC MMC Property-sheet extension
{2797CF92-415A-43e6-A8F7-A5FAAB783719} CPartitionPropPages Class
{2C3E140B-7A0D-42d1-B2AA-D343500A90CF} CTrkEvtListener Class
{2f893820-7089-46cc-a6e8-c4aae45f151b} DTC MMC Snap-in
{410381DB-AF42-11D1-8F10-00C04FC2C17B} COMNSView Class
{838A77A6-14D4-439C-925F-30EE58005026} CCOMNSScopeForExtensionSnapin Class
{8C836AF9-FFAC-11D0-8ED4-00C04FC2C17B} ReplicateCatalog Class
{9305969B-F45F-47e5-A954-6EA879E874CC} CPartitionSetPropPages Class
{99847C33-B1B4-11D1-8F10-00C04FC2C17B} CCOMNSScopeImpl Class
{9cfc6d75-e648-47a8-9ea0-fb0907558952} DTC Transaction List Control
{a00e1768-4a9b-4d97-afc6-99d329f605f2} CPartitionNotify Class
{AB790AA1-CDC1-478a-9351-B2E05CFCAD09} CPartitionContextMenu Class
{C9BC92DF-5B9A-11D1-8F00-00C04FC2C17B} ComponentDataImpl Class
{D7FCB63B-5C55-11D1-8F00-00C04FC2C17B} SnapinAboutImpl Class
{DFFFAE4D-F0CF-46CD-9586-FE891237AB8A} ComponentServicesExtensionSnapin Class
{EEBD2F15-87EE-4f93-856F-6AD7E31787B3} CPartitionSetContextMenu Class
{FA3E1D55-16DF-446d-872E-BD04D4F39C93} CUserPropPages Class
Tue Jul 14 04:53:50 2009 Z
{0CF32AA1-7571-11D0-93C4-00AA00A3DDEA} System Monitor Source Properties
{1d27f844-3a1f-4410-85ac-14651078412d} CompatContextMenu Class
{513D916F-2A8E-4F51-AEAB-0CBC76FB1AF8} LayerUIPropPage
{7478EF61-8C46-11d1-8D99-00A0C913CAD4} ComponentData Class
{7478EF65-8C46-11d1-8D99-00A0C913CAD4} ComponentData Class
{7478EF69-8C46-11d1-8D99-00A0C913CAD4} PerformanceAbout Class
{74b077e8-32de-40ab-be4e-65609f575459} Resource Monitor
{855fec53-d2e4-4999-9e87-3414e9cf0ff4} RunTask
{C3E5D3D2-1A03-11CF-942D-008029004347} System Monitor General Properties
{C3E5D3D3-1A03-11CF-942D-008029004347} System Monitor Graph Properties
{C4D2D8E0-D1DD-11CE-940F-008029004347} System Monitor Control
{CF948561-EDE8-11CE-941E-008029004347} System Monitor Data Properties
{D3075F87-A7BD-4231-9F6A-60C5E07374A7}
{E49741E9-93A8-4AB1-8E96-BF4482282E9C} System Monitor Appearance Properties
Tue Jul 14 04:53:49 2009 Z
{06587E71-F043-403A-BF49-CB591BA6E103} AudioVolume Class
{07252659-bb6b-4b79-b78b-623f6699a579} AudioConstrictor Class
{0E681C52-CD03-11D2-8853-0000F80883E3}
{101193C0-0BFE-11D0-AF91-00AA00B67A42} Display

```

## SOFTWARE OUTPUT

{1206F5F1-0569-412C-8FEC-3204630DFB70} Credential Manager  
 {129D7E40-C10D-11D0-AFB9-00AA00B67A42} DV Muxer  
 {12DD4DBB-532B-4FCE-8653-74CDB9C8FE5A} AudioMixer Class  
 {13AA3650-BB6F-11D0-AFB9-00AA00B67A42} DV Video Encoder  
 {1FE45ED3-B842-4CF2-8DF6-43E3D6D10E64} audiokscaptureendpoint class  
 {20404060-F24F-4F89-84C6-8AF80B0A17CB} AudioKSRenderEndpoint Class  
 {27c98999-2895-4829-b080-5a8b65bd3db0} AudioRateConvertCMPT Class  
 {294935CE-F637-4E7C-A41B-AB255460B862}  
 {2968B3C3-CC07-40BE-B78F-094B7C310479}  
 {3BF043EF-A974-49B3-8322-B853CF1E5EC5} Microsoft VolumeControlService Class  
 {3DC09436-7D83-4BA0-ADDC-CD47F996C5BA} AudioMeter Class  
 {3fd7f233-a716-472e-8f2f-c25954f34e96} AudioFormatConvert Class  
 {3FF23902-CD1F-11D2-8853-0000F80883E3}  
 {4150F050-BB6F-11D0-AFB9-00AA00B67A42} Format  
 {41FCCC3A-1FA1-4949-953A-6EE61C46A4D1} Microsoft.Audio.AudioClient Binder  
 {49c47ce0-9ba4-11d0-8212-00c04fc32c45} SFilter Class  
 {49C47CE4-9BA4-11D0-8212-00C04FC32C45} Stream Class  
 {49c47ce5-9ba4-11d0-8212-00c04fc32c45} MMStream Class  
 {4EB31670-9FC6-11CF-AF6E-00AA00B67A42} DV Splitter  
 {503739d0-4c5e-4cfd-b3ba-d881334f0df2} VaultCredProvider  
 {525C410E-B007-4F15-81DD-49DF9B17139B}  
 {541987EE-0E02-411E-9A85-1FC6156E7F4B} audiomatrix class  
 {565DCEF2-AFC5-11D2-8853-0000F80883E3}  
 {5BFD515E-4ABA-4483-A1C5-6651B7110AB6} CrossProcessServerOutputEndpoint Class  
 {75269C13-41E1-4D0E-B8A0-9F8F22E246C9} SystemAudioDeviceExclusive Class  
 {7FF0997A-1999-4286-A73C-622B8814E7EB} ICodecAPIProxy  
 {8496e040-af4c-11d0-8212-00c04fc32c45} AuStream Class  
 {870AF99C-171D-4f9e-AF0D-E63DF40C2BC9}  
 {888D5481-CABB-11D1-8505-00A0C91F9CA0} VideoRenderCtl Class  
 {89115307-8248-448f-ADA0-F3F3718A9B2A} SystemAudioDeviceShared Class  
 {948CFD8C-1888-4E52-8703-99610347EBB6} AudioPump Class  
 {9B8C4620-2C1A-11D0-8493-00A02438AD48} DVD Navigator  
 {9DBA709C-B3E1-4013-95B7-5ED33A2E8561} CrossProcessServerInput Class  
 {A73BEEB2-B0B7-11D2-8853-0000F80883E3}  
 {ADD18BF7-AB60-4283-A580-D7544DD255D2} AudioDeviceGraph Class  
 {B05DABD9-56E5-4FDC-AFA4-8A47E91F1C9C} IVideoEncoderCodecAPIProxy  
 {B1B77C00-C3E4-11CF-AF79-00AA00B67A42} DV Video Decoder  
 {B43C4EEC-8C32-4791-9102-508ADA5EE8E7} IVideoEncoderProxy  
 {C58BD103-E87F-4B78-A0FA-7A5C95970EE2} AudioRateConvert Class  
 {CD773740-B187-4974-A1D5-E0FF91372277} CrossProcessClientOutput Class  
 {CF0F2F7C-F7BF-11d0-900D-00C04FD9189D} MtStream Class  
 {d69e0717-dd4b-4b25-997a-da813833b8ac} AudioLimiter Class  
 {E1150CE9-5BD4-4044-8FE9-98CF40137A41} AudioProcessor Class  
 {e916b6b2-22bd-4afc-b337-d3d9fb27670e} AudioCopy Class  
 {f2468580-af8a-11d0-8212-00c04fc32c45} AuStream Class  
 {F2DDFC82-8F12-4CDD-B7DC-D4FE1425AA4D} Sound Control Panel  
 {F64A6DA6-E8AF-4B7B-BCA8-847AE765D538} CrossProcessClientInputEndpoint class  
 {F963C5CF-A659-4A93-9638-CAF3CD277D13} DVD State

## SOFTWARE OUTPUT

{FAC67227-E178-4fab-9FEA-B4E77D3DBE7D} Video Extension Class  
 {FCC152B7-F372-11D0-8E00-00C04FD7C08B} DVD Graph Builder  
 {FD7F2B29-24D0-4B5C-B177-592C39F9CA10} psfactorybuffer  
 Tue Jul 14 04:53:48 2009 Z  
 {7444C717-39BF-11D1-8CD9-00C04FC29D45} CryptPKO Class  
 {7444C719-39BF-11D1-8CD9-00C04FC29D45} CryptSig Class  
 {B9F8AC3E-0F71-11D2-B72C-00C04FB6BD3D} Ks IBasicAudio Interface Handler  
 Tue Jul 14 04:53:47 2009 Z  
 {148BD520-A2AB-11CE-B11F-00AA00530503} Scheduling Agent Task Object Class  
 {148BD52A-A2AB-11CE-B11F-00AA00530503} Scheduling Agent Service Class  
 {3c6859ce-230b-48a4-be6c-932c0c202048} Sxs Store Class  
 {4729dc2b-36ff-405f-bd36-f45113adb052} Component Based Servicing Retry Session  
 {75207391-23F2-4396-85F0-8FDB879ED0ED} Component Based Servicing Session  
 Proxy/Stub  
 {752073A1-23F2-4396-85F0-8FDB879ED0ED} Component Based Servicing Session  
 {8601319a-d7cf-40f3-9025-7f77125453c6} Sxs Store Class Proxy/Stub  
 {8F5DF053-3013-4dd8-B5F4-88214E81C0CF} SFP Repair Class  
 {90ED9FAA-A6E5-4671-8E50-1C060F8B9C47} SFP Interface Class  
 {A65B8071-3BFE-4213-9A5B-491DA4461CA7} DxDiagProvider Class  
 Tue Jul 14 04:53:46 2009 Z  
 {01575CFE-9A55-4003-A5E1-F38D1EBDCBE1} MsCtfMonitor task handler  
 {05238C14-A6E1-11D0-9A84-00C04FD8DBF7} PSFactoryBuffer  
 {1B1A897E-FBEE-41CF-8C48-9BF764F62B8B} SoftKbd Class  
 {3318360C-1AFC-4D09-A86B-9F9CB6DCEB9C} ClassicLangBar  
 {394C052E-B830-11D0-9A86-00C04FD8DBF7}   
 {4955DD33-B159-11D0-8FCF-00AA006BCC59} CActiveIMMApp  
 {50D5107A-D278-4871-8989-F4CEAAF59CFC} CActiveIMMAppEx\_Trident  
 {540D8A8B-1C3F-4E32-8132-530F6A502090} Language bar  
 {5C659257-E236-11D2-8899-00104B2AFB46} WMISnapin Class  
 {5C659258-E236-11D2-8899-00104B2AFB46} Allows configuration and control of the  
 Windows Management Instrumentation (WMI) service.  
 {6A49950E-CE8A-4EF7-88B4-9D112366511C} SoftKbdRegistry Class  
 {93AC9CB8-27D5-4482-BFDF-68F21C7454A3} Microsoft Shared Correction UI  
 {975797FC-4E2A-11D0-B702-00C04FD8DBF7}   
 {A1B9E04A-3226-11D2-883E-00104B2AFB46} SDSnapin Description  
 {AE6BE008-07FB-400D-8BEB-337A64F7051F} TF\_TransitoryExtensionUIEntry  
 {B5F8FB3B-393F-4F7C-84CB-504924C2705A} PSFactoryBuffer  
 {BD95BA60-2E26-AAD1-AD99-00AA00B8E05A} SDSnapin Class  
 {C1EE01F2-B3B6-4A6A-9DDD-E988C088EC82} CActiveIMMAppEx  
 {E429B25A-E5D3-4D1F-9BE3-0C608477E3A1} Table Driven Text Input Processor  
 {F778C6B4-C08B-11D2-976C-00C04F79DB19}   
 {F89E9E58-BD2F-4008-9AC2-0F816C09F4EE} SoftKbdIMX Class  
 Tue Jul 14 04:53:45 2009 Z  
 {0725C3CB-FEFB-11D0-99F9-00C04FC2F8EC} WDM Event Provider  
 {172BDDF8-CEEA-11D1-8B05-00600806D9B6} Wbem Scripting Object Path  
 {1EF94880-01A8-11D2-A90B-00AA00BF3363} Microsoft NT DS Class Provider for WBEM  
 {23B77E99-5C2D-482D-A795-62CA3AE5B673} WBEM IP Route Provider  
 {266C72D4-62E8-11D1-AD89-00C04FD8FDFF} Microsoft WBEM Log File Event Consumer



## SOFTWARE OUTPUT

Provider  
 {266C72E5-62E8-11D1-AD89-00C04FD8FDFF} Microsoft WBEM Command Line Event Consumer  
 Provider  
 {266C72E6-62E8-11D1-AD89-00C04FD8FDFF} Microsoft WBEM NT Event Log Event Consumer  
 Provider  
 {266C72E7-62E8-11D1-AD89-00C04FD8FDFF} Microsoft WBEM Active Scripting Event  
 Consumer Provider  
 {33831ED4-42B8-11D2-93AD-00805F853771} Microsoft NT DS Class Associations  
 Provider for WBEM  
 {35B78F79-B973-48C8-A045-CAEC732A35D5} WDM HiPerf Provider  
 {443C8934-90FF-48ED-BCDE-26F5C7450042} PSFactoryBuffer  
 {47DFBE54-CF76-11D3-B38F-00105A1F473A} WBEM Scripting DateTime  
 {54B50739-686F-45EB-9DFF-D6A9A0FAA9AF} PSFactoryBuffer  
 {5791BC26-CE9C-11D1-97BF-0000F81E849C} WBEM Scripting Object Path  
 {5CE34C0D-0DC9-4C1F-897C-DAA1B78CEE7C} PSFactoryBuffer  
 {6515834D-6125-4878-A3A3-6B0A73B809A2} Win32\_JobObjectLimitInfo Component  
 {659CDEAD-489E-11D9-A9CD-000D56965251} PSFactoryBuffer  
 {659CDEAE-489E-11D9-A9CD-000D56965251} psfactorybuffer  
 {6D7A4B0E-66D5-4AC3-A7ED-0189E8CF5E77} WBEM IP Route Event Provider  
 {72967901-68EC-11D0-B729-00AA0062CBB7} WBEM Registry Property Provider  
 {72967903-68EC-11D0-B729-00AA0062CBB7} WBEM PerfMon Property Provider  
 {734AC5AE-68E1-4FB5-B8DA-1D92F7FC6661} WBEM Ping Provider  
 {75718C9A-F029-11D1-A1AC-00C04FB6C223} WBEM Scripting Sink  
 {76A64158-CB41-11D1-8B02-00600806D9B6} WBEM Scripting Locator  
 {7FB1D98A-F895-4761-8DC2-774969C84D10} Win32\_JobObject Provider Component  
 {9877D8A7-FDA1-43F9-AEEA-F90747EA66B0} KernelTraceProvider Class  
 {9a2584c3-f7d2-457a-9a5e-22b67bffc7d2} psfactorybuffer  
 {9AED384E-CE8B-11D1-8B05-00600806D9B6} WBEM Scripting Named Value Collection  
 {AA527A40-4D9A-11D2-93AD-00805F853771} Microsoft NT DS Instance Provider for WBEM  
 {AA70DDF4-E11C-11D1-ABB0-00C04FD9159E} Microsoft WBEM View Provider  
 {AB40A5C1-804B-40BD-9DFE-A640691C6956} Win32\_JobObjectSecLimitInfo Component  
 {BE0A9830-2B8B-11D1-A949-0060181EBBAD} WMI MSI Provider  
 {C0AA9D93-2EF5-47FB-960C-F90FC644B48E} Win32\_JobObjectIOAccountingInfo Component  
 {C2FEEEEAC-CFCD-11D1-8B05-00600806D9B6} Wbem Scripting Last Error  
 {C4819C8D-9AB8-4B2F-B8AE-C77DABF553D5} Microsoft WBEM Current Time Provider  
 {C7A3A54B-0250-11D3-9CD1-00105A1F4801} Microsoft WBEM SMTP Event Consumer  
 Provider  
 {D269BF5C-D9C1-11D3-B38F-00105A1F473A} WBEM Scripting Refresher  
 {D2D588B5-D081-11D0-99E0-00C04FC2F8EC} WDM Instance Provider  
 {ef7e0655-7888-4960-b0e5-730846e03492} psfactorybuffer  
 {F00B4404-F8F1-11CE-A5B6-00AA00680C3F} WBEM PerfMon Instance Provider  
 {f1bd1079-9f01-4bdc-8036-f09b70095066} psfactorybuffer  
 {F55C5B4C-517D-11D1-AB57-00C04FD9159E} Microsoft WBEM NT Eventlog Event Provider  
 {FA77A74E-E109-11D0-AD6E-00C04FD8FDFF} WBEM Registry Event Provider  
 {FD4F53E0-65DC-11D1-AB64-00C04FD9159E} Microsoft WBEM NT Eventlog Instance  
 Provider  
 {FE9AF5C0-D3B6-11CE-A5B6-00AA00680C3F} WBEM Registry Instance Provider  
 Tue Jul 14 04:53:43 2009 Z

## SOFTWARE OUTPUT

```

{066D2323-D35A-4C15-AE22-F88F136C1613} KeystrokeGenerator Class
{0A56CD6C-B45A-4A6C-A88C-3F42AC7BCED4} KeyStrokeMonitor Class
{220A0D48-03A8-4F7B-8408-4EB506EF68D9} PSFactoryBuffer
{632B0530-3CBF-44F4-BFDC-750A80D4B00A} StateController Class
{634F8410-E924-46B8-A1B5-E8B08E8B8750} PSFactoryBuffer
{68904ac7-1801-47f8-af3a-dac14848fd75} PSFactoryBuffer
{6A514DB9-3EC1-4F36-9F95-BC0B00152D0B} DefinitionParser Class
{6af6b181-3a90-4fac-9655-b34041d46b8f} PSFactoryBuffer
{884CFF4F-0BB0-4CAA-83BD-4FB9ECE938FA} DefinitionLoader Class
{BFC7DC7B-8F11-4A40-8DB2-207302E2D61B} PSFactoryBuffer
{E13B9A7F-EC39-4E7F-9970-12F348C89FD0} PSFactoryBuffer
{E787250A-F3B3-4e8d-A300-F58FB129B709} PSFactoryBuffer
{E800E945-780D-48D3-89E7-D822EA18F0A2} PSFactoryBuffer
{F3252D7B-E51D-4B14-AA5E-8E3D4315F73C} PSFactoryBuffer

```

Tue Jul 14 04:53:38 2009 Z

```

CLSID {0000031A-0000-0000-C000-000000000046}
{0000002F-0000-0000-C000-000000000046} CLSID_RecordInfo
{00000300-0000-0000-C000-000000000046} StdOleLink
{00000301-A8F2-4877-BA0A-FD2B6645FB94} PSFactoryBuffer
{00000303-0000-0000-C000-000000000046} FileMoniker
{00000304-0000-0000-C000-000000000046} ItemMoniker
{00000305-0000-0000-C000-000000000046} AntiMoniker
{00000306-0000-0000-C000-000000000046} PointerMoniker
{00000308-0000-0000-C000-000000000046} PackagerMoniker
{00000309-0000-0000-C000-000000000046} CompositeMoniker
{0000030B-0000-0000-C000-000000000046} DfMarshal
{00000315-0000-0000-C000-000000000046} Picture (Metafile)
{00000316-0000-0000-C000-000000000046} Picture (Device Independent Bitmap)
{00000319-0000-0000-C000-000000000046} Picture (Enhanced Metafile)
{0000031A-0000-0000-C000-000000000046} ClassMoniker
{0000031D-0000-0000-C000-000000000046} DCOMAccessControl
{00000320-0000-0000-C000-000000000046} PSFactoryBuffer
{00000327-0000-0000-C000-000000000046} objref
{0000032E-0000-0000-C000-000000000046} PipePSFactory
{00000507-0000-0010-8000-00AA006D2EA4} ADODB.Command
{0000050B-0000-0010-8000-00AA006D2EA4} ADODB.Parameter
{00000514-0000-0010-8000-00AA006D2EA4} ADODB.Connection
{0000051A-0000-0010-8000-00AA006D2EA4} ADO 6.0
{00000535-0000-0010-8000-00AA006D2EA4} ADODB.Recordset
{00000541-0000-0010-8000-00AA006D2EA4} ADODB.Error
{00000542-0000-0010-8000-00AA006D2EA4} ADODB Error Lookup Service
{00000560-0000-0010-8000-00AA006D2EA4} ADODB.Record
{00000566-0000-0010-8000-00AA006D2EA4} ADODB.Stream
{00000602-0000-0010-8000-00AA006D2EA4} ADOX.Catalog.6.0
{00000609-0000-0010-8000-00AA006D2EA4} ADOX.Table.6.0
{00000615-0000-0010-8000-00AA006D2EA4} ADOX.Group.6.0
{00000618-0000-0010-8000-00AA006D2EA4} ADOX.User.6.0
{0000061B-0000-0010-8000-00AA006D2EA4} ADOX.Column.6.0

```

## SOFTWARE OUTPUT

```

{0000061E-0000-0010-8000-00AA006D2EA4} ADOX.Index.6.0
{00000621-0000-0010-8000-00AA006D2EA4} ADOX.Key.6.0
{00020000-0000-0000-C000-000000000046} Microsoft AVI Files
{00020001-0000-0000-C000-000000000046} AVI Compressed Stream
{00020003-0000-0000-C000-000000000046} Microsoft Wave File
{0002000D-0000-0000-C000-000000000046} IAVIStream & IAVIFile Proxy
{0002000F-0000-0000-C000-000000000046} ACM Compressed Audio Stream
{00020420-0000-0000-C000-000000000046} PSDispatch
{00020421-0000-0000-C000-000000000046} PSEnumVariant
{00020422-0000-0000-C000-000000000046} PSTypeInfo
{00020423-0000-0000-C000-000000000046} PSTypeLib
{00020424-0000-0000-C000-000000000046} PSOAInterface
{00020425-0000-0000-C000-000000000046} PSTypeComp
{00020810-0000-0000-C000-000000000046}
{00020811-0000-0000-C000-000000000046}
{00020820-0000-0000-C000-000000000046}
{00020821-0000-0000-C000-000000000046}
{00020900-0000-0000-C000-000000000046}
{00020906-0000-0000-C000-000000000046}
{00020D75-0000-0000-C000-000000000046}
{00021400-0000-0000-C000-000000000046} Desktop
{00021401-0000-0000-C000-000000000046} Shortcut
{0002E005-0000-0000-C000-000000000046} Component Categories Manager
{0002E006-0000-0000-C000-000000000046} Component Categories Manager With Class
Store
{000C101C-0000-0000-C000-000000000046} Msi install server
{000C101D-0000-0000-C000-000000000046} Microsoft Windows Installer Message RPC
{000C103E-0000-0000-C000-000000000046} PSFactoryBuffer
{000C1090-0000-0000-C000-000000000046} Microsoft Windows Installer
{000C1094-0000-0000-C000-000000000046}
{0010668C-0801-4DA6-A4A4-826522B6D28F}
{00108226-EE41-44A2-9E9C-4BE4D5B1D2CD}
{0010890e-8789-413c-adbc-48f5b511b3af} User Notification
{00393519-3A67-4507-A2B8-85146167ACA7} WPD Association LUA Virtual Factory
{003e0278-eca8-4bb8-a256-3689ca1c2600} Published Items Shell Service Object
{00597829-82CE-44d4-8B0B-40BE695973B5} WMPDMCServersManager Class
{006E61DF-1A43-4F2C-B26F-780BAEA3A92D}
{0086c339-9c0e-4c09-9a2f-ff3d19a44a18} PSFactoryBuffer
{009f3b45-8a6b-4360-b997-b2a009a16402} XWizard Factory Generated Class (HomeGroup
Update Passkey/Merge Hook Page)
{00BB2763-6A77-11D0-A535-00C04FD7D062} Microsoft AutoComplete
{00BB2764-6A77-11D0-A535-00C04FD7D062} Microsoft History AutoComplete List
{00BB2765-6A77-11D0-A535-00C04FD7D062} Microsoft Multiple AutoComplete List
Container
{00da2f99-f2a6-40c2-b770-a920f8e44abc} Staging ShellFolder for CD Burning
{00eebf57-477d-4084-9921-7ab3c2c9459d} CD Burn Merged Folder
{00f20eb5-8fd6-4d9d-b75e-36801766c8f1} PhotoAcqDropTarget
{00f210a1-62f0-438b-9f7e-9618d72a1831} PhotoAcquireOptionsDialog

```

## SOFTWARE OUTPUT

{00f24ca0-748f-4e8a-894f-0e0357c6799f} PhotoProgressDialog  
 {00f26e02-e9f2-4a9f-9fdd-5a962fb26a98} PhotoAcquire  
 {00f29a34-b8a1-482c-bcf8-3ac7b0fe8f62} PhotoAcqDeviceSelectionDlg  
 {00f2b433-44e4-4d88-b2b0-2698a0a91dba} PhotoAcqHwEventHandler  
 {00F2CE1E-935E-4248-892C-130F32C45CB4} PSFactoryBuffer  
 {0102563D-F16D-434d-82A2-37968BD3E31E} RNWF Extensible Helper Class  
 {011B3619-FE63-4814-8A84-15A194CE9CE3} WebDVD Device Segment  
 {0131BE10-2001-4C5F-A9B0-CC88FAB64CE8}  
 {0142e4d0-fb7a-11dc-ba4a-000ffe7ab428} Biometrics  
 {0142e4d1-fb7a-11dc-ba4a-000ffe7ab428} Virtual Factory for Biometrics  
 {0142e4d2-fb7a-11dc-ba4a-000ffe7ab428}  
 {0142e4d3-fb7a-11dc-ba4a-000ffe7ab428}  
 {01458CF0-A1A2-11D1-8F85-00600895E7D5} Interface Proxy Stub  
 {0149EEDF-D08F-4142-8D73-D23903D21E90} XDS Feature Segment  
 {01822ABA-23F0-4506-9BBC-680F5D6D606C} CLSID\_ContactUserAccountChangeCallback  
 {01A3BF5C-CC93-4C12-A4C3-09B0BBE7F63F}  
 {01afc156-f2eb-4c1c-a722-8550417d396f} Action Center PSFactory  
 {01CBCF66-A9CA-4449-84DE-7F321232BBC7} html persistent handler for mapi email  
 {01E04581-4EEE-11d0-BFE9-00AA005B4383} &Address  
 {01F36CE2-0907-4d8b-979D-F151BE91C883} CFrameRateConvertDmo  
 {021003e9-aac0-4975-979f-14b5d4e717f8} LocalCopyHelper  
 {02805F1E-D5AA-415B-82C5-61C033A988A6}  
 {02df6db6-9405-4812-b3f6-500e8615b7af} Registry Data Driven Command  
 {03012959-F4F6-44D7-9D09-DAA087A9DB57}  
 {03022430-ABC4-11D0-BDE2-00AA001A1953} PSFactoryBuffer  
 {031E4825-7B94-4dc3-B131-E946B44C8DD5} UsersLibraries  
 {031EE060-67BC-460d-8847-E4A7C5E45A27} Windows Media Player Rich Preview Handler  
 {0344ec28-5339-4124-a186-2e8eef168785} MFSourceFilter  
 {0369B4E5-45B6-11D3-B650-00C04F79498E} BDA Tuning Model Channel Tune Request  
 {0369B4E6-45B6-11D3-B650-00C04F79498E} BDA Tuning Model ATSC Channel Tune Request  
 {036A9790-C153-11D2-9EF7-006008039E37} Audio Mixer  
 {03837511-098B-11D8-9414-505054503030} TraceDataProviderCollection  
 {03837513-098B-11D8-9414-505054503030} TraceDataProvider  
 {0383751C-098B-11D8-9414-505054503030} TraceSession  
 {03837521-098B-11D8-9414-505054503030} DataCollectorSet  
 {03837525-098B-11D8-9414-505054503030} DataCollectorSetCollection  
 {03837526-098B-11D8-9414-505054503030} LegacyDataCollectorSet  
 {03837527-098B-11D8-9414-505054503030} LegacyDataCollectorSetCollection  
 {03837528-098B-11D8-9414-505054503030} LegacyTraceSession  
 {03837529-098B-11D8-9414-505054503030} LegacyTraceSessionCollection  
 {03837530-098B-11D8-9414-505054503030} TraceSessionCollection  
 {03837531-098B-11D8-9414-505054503030} ServerDataCollectorSet  
 {03837532-098B-11D8-9414-505054503030} ServerDataCollectorSetCollection  
 {03837538-098B-11D8-9414-505054503030} BootTraceSession  
 {03837539-098B-11D8-9414-505054503030} BootTraceSessionCollection  
 {03837546-098B-11D8-9414-505054503030} ServerDataCollectorSet  
 {03837547-098B-11D8-9414-505054503030} SystemDataCollectorSetCollection  
 {03A0E2CD-23A9-45ed-968F-6FDA22B2285E} New Network Category Custom Page

## SOFTWARE OUTPUT

{03C036F1-A186-11D0-824A-00AA005B4383} Microsoft Shell Folder AutoComplete List  
 {03C06416-D127-407A-AB4C-FDD279ABBE5D} BDA Tuning Model Digital Cable Locator  
 {03ca98d6-ff5d-49b8-abc6-03dd84127020} Background Intelligent Transfer Control

Class 2.5

{03e15b2e-cca6-451c-8fb0-1e2ee37a27dd} CTapiluaLib Class  
 {0429EC6E-1144-4bed-B88B-2FB9899A4A3D} Custom Composition Segment from Data

Services to XDS

{042dc17c-023f-43df-a3ec-982b4dc78a64} Schema Migration Plugin  
 {04731B67-D933-450a-90E6-4ACD2E9408FE} CLSID\_SearchFolder  
 {04788120-12C2-498D-83C1-A7D92E677AC6} WBEM Framework Instance Provider CIMA  
 {0482DDE0-7817-11CF-8A03-00AA006ECB65} KsDataTypeHandlerAnalogVideo  
 {0482E074-C5B7-101A-82E0-08002B36A333}  
 {04a1e553-fe36-4fde-865e-344194e69424} Microsoft InkPicture Control  
 {04A578B2-E778-422A-A805-B3EE54D90BD9} PSFactoryBuffer  
 {04B55BC3-33DE-4d79-94EC-830CDF96CC82} WMPPlayer ContentPropPage Class  
 {04FBCBF4-DC23-3CEC-9025-9D4093C26733}  
 {0520af9e-e3da-4b32-8be8-0f3e475bfc5f} Device Center Print Status Extension  
 {05300401-BCBC-11d0-85E3-00C04FD85AB4} MHTML Asynchronous Pluggable Protocol

Handler

{05589F80-C356-11CE-BF01-00AA0055595A} KsDataTypeHandlerVideo  
 {05589FA1-C356-11CE-BF01-00AA0055595A} ActiveMovieControl Object  
 {05589FAF-C356-11CE-BF01-00AA0055595A} Audio Renderer Property Page  
 {055CB2D7-2969-45CD-914B-76890722F112} BDA Tuning Model MPEG2 Component Class

(Broadcast Substream)

{056440FD-8568-48e7-A632-72157243B55B} Explorer Navigation Bar  
 {05DF8D13-C355-47f4-A11E-851B338CEFB8} CQueryAllWinSAT Class  
 {05F3561D-0358-4687-8ACD-A34D24C488DF} Health Center Control Panel  
 {060AF76C-68DD-11D0-8FC1-00C04FD9189D} Seeking  
 {06290BD0-48AA-11D2-8432-006008C3FBFC} Object under which scriptlets may be

created

{06290BD1-48AA-11D2-8432-006008C3FBFC} Constructor that allows hosts better

control creating scriptlets

{06290BD2-48AA-11D2-8432-006008C3FBFC} Factory bindable using IPersistMoniker  
 {06290BD3-48AA-11D2-8432-006008C3FBFC} Moniker to a Windows Script Component  
 {06290BD4-48AA-11D2-8432-006008C3FBFC} Object for encoding scriptlets  
 {06290BD5-48AA-11D2-8432-006008C3FBFC} Object for constructing type libraries for

scriptlets

{06290BD8-48AA-11D2-8432-006008C3FBFC} Constructor for Scriptlet Automation

Handler

{06290BD9-48AA-11D2-8432-006008C3FBFC} Constructor for Scriptlet Event Handler  
 {06290BDA-48AA-11D2-8432-006008C3FBFC} Constructor for Scriptlet ASP Handler  
 {06290BDB-48AA-11D2-8432-006008C3FBFC} Constructor for Scriptlet Behavior Handler  
 {063B79F5-7539-11D2-9773-00A0C9B4D50C} Microsoft COM+ Services Meta Data  
 {063B79F6-7539-11D2-9773-00A0C9B4D50C} Microsoft COM+ Services Meta Data  
 {06622D85-6856-4460-8DE1-A81921B41C4B} COpenControlPanel  
 {067B4B81-B1EC-489f-B111-940EBDC44EBE} WMDM CE Device Service Provider  
 {06A03425-C9EB-11d2-8CAA-0080C739E3E0} Help Collection Wrapper Class  
 {06B32AEE-77DA-484B-973B-5D64F47201B0} VMR Mixer

## SOFTWARE OUTPUT

```

{06C792F8-6212-4F39-BF70-E8C0AC965C23} User Account Control Settings
{06CCA63E-9941-441B-B004-39F999ADA412} MMEndpointManager class
{06EEE695-542D-46F6-AEAB-FA2F1B2102D3} GameCleanupHandler Class
{0700F42F-EEE3-443a-9899-166F16286796} HomeGroup Network
{07398dcf-2e0b-4ece-99dd-56b262db948b} Search Protocol URL Generator
{078759d3-423b-48ad-ab6a-5638c2884dbe} Shell Undo Parent Unit
{079AA557-4A18-424A-8EEE-E39F0A8D41B9} SAX XML Reader
{07A774A0-6047-11D1-BA20-006097D2898E} Logagent Class
{07AA0886-CC8D-4e19-A410-1C75AF686E62} Onex PLAP Credential Provider
{07B65360-C445-11CE-AFDE-00AA006C14F4} MIDI Renderer
{07D26616-6136-11D1-8C9C-00C04FC3261D}
{080d0d78-f421-11d0-a36e-00c04fb950dc} ADs LDAP Pathname Descriptor Object
{08244EE6-92F0-47f2-9FC9-929BAA2E7235} Sharing Overlay (Private)
{083863F1-70DE-11D0-BD40-00A0C911CE86} ActiveMovie Filter Class Manager
{08a99e2f-6d6d-4b80-af5a-baf2bcbe4cb9} PropVariantCollection Class
{08d5bfbf-fbca-4322-9f70-ca9f66f8ed6a} CommonLayoutModifier
{09017262-fdb4-4ff2-9013-26332c926ee7} Csc Sync
{09144FD6-BB29-11DB-96F1-005056C00008} PBDA DTFilter
{093FF999-1EA0-4079-9525-9614C3504B74} Windows Script Host Network Object
{09474572-B2FB-11D1-A1A1-0000F875B132} MMCListPadInfo class
{0955AC62-BF2E-4CBA-A2B9-A63F772D46CF} BDA Tuning Model MPEG2 Tune Request
{0977EEC5-10F7-44AE-A7FA-D4824EBA5C74} PrintersCacheManager Class
{09799AFB-AD67-11d1-ABCD-00C04FC30936} Open With Context Menu Handler
{098f2470-bae0-11cd-b579-08002b30bfeb} Null persistent handler
{0997898B-0713-11d2-A4AA-00C04F8EEB3E} Common Places FS Folder
{09a28848-0e97-4cef-b950-cea037161155} Remove Properties Drop Target
{09C20568-F30C-489B-AE9C-4930AD7F165F} PSFactoryBuffer
{09DBBC77-588F-4517-A485-74A29759F54C} PSFactoryBuffer
{0A16D195-6F47-4964-9287-9F4BAB6D9827} PSFactoryBuffer
{0A29F9BD-86B3-4384-B25D-EF1FFE020266} WSD Scan Proxy
{0A522732-A626-11D0-8D60-00C04FD6202B} CLSID_CExchImport
{0A886F29-465A-4aea-8B8E-BE926BFAE83E} EapQecMessenger
{0A88C858-7D0C-4549-9499-7DB05F0CB0BF} Share Home Group
{0A9AE910-85C0-11D0-BD42-00A0C911CE86} AVI mux Property Page1
{0AA02E8D-F851-4CB0-9F64-BBA9BE7A983D} AlchemyVis Class
{0AE89F03-C538-4471-9B12-A8E8EF246A0D} PSFactoryBuffer
{0af10cec-2ecd-4b92-9581-34f6ae0637f3} PortableDeviceManager Class
{0af96ede-aebf-41ed-a1c8-cf7a685505b6} Library Folder Context Menu
{0AFACED1-E828-11D1-9187-B532F1E9575D} Folder Shortcut
{0AFCCBA6-BF90-4A4E-8482-0AC960981F5B}
{0B124F8F-91F0-11D1-B8B5-006008059382} Installed Apps Enumerator
{0b2feecb-1577-4fa6-9a29-bd9022ebcf90} CPPTPDiaHelper Object
{0B3FFB92-0919-4934-9D5B-619C719D0202} Broadcast Event Service
{0B5A7836-4C16-4560-90B2-0F5DAF6D6D1B} FormHost Class
{0b91a74b-ad7c-4a9d-b563-29eef9167172} WpdSerializer Class
{0BA2A2AC-A4D5-38CB-AD03-A0D5B6EC4646}
{0BE35200-8F91-11CE-9DE3-00AA004BB851} Font Property Page
{0BE35201-8F91-11CE-9DE3-00AA004BB851} Color Property Page

```

## SOFTWARE OUTPUT

{0BE35202-8F91-11CE-9DE3-00AA004BB851} Picture Property Page  
 {0BE35203-8F91-11CE-9DE3-00AA004BB851} Standard Font  
 {0BE35204-8F91-11CE-9DE3-00AA004BB851} Standard Picture  
 {0BFCF7B7-E7B6-433a-B205-2904FCF040DD} New Shortcut Wizard Modal  
 {0c15d503-d017-47ce-9016-7b3f978721cc} PortableDeviceValues Class  
 {0C39A5CF-1A7A-40C8-BA74-8900E6DF5FCD}  
 {0C3B05FB-3498-40C3-9C03-4B22D735550C} RasDlg LUA  
 {0C5672F9-3EDC-4b24-95B5-A6C54C0B79AD} Rational Class  
 {0C776A5A-FC42-4870-8D65-D62ADD9184FF} Magic USB Cable Class ID  
 {0cbb5030-f2b2-4b38-8cbc-895cec57db03} Create 802.11 Ad hoc Task Class  
 {0cbb5031-f2b2-4b38-8cbc-895cec57db03} Adhoc Create Adapter Selection Page Class  
 {0cbb5032-f2b2-4b38-8cbc-895cec57db03} Adhoc Create Setup Page Class  
 {0cbb5034-f2b2-4b38-8cbc-895cec57db03} Adhoc Create Status Page Class  
 {0cbb5035-f2b2-4b38-8cbc-895cec57db03} Adhoc Create Finish Page Class  
 {0cbb5036-f2b2-4b38-8cbc-895cec57db03} Adhoc Ics Option Page Class  
 {0cbb5037-f2b2-4b38-8cbc-895cec57db03} Adhoc Ics Status Page Class  
 {0cbb5038-f2b2-4b38-8cbc-895cec57db03} Adhoc Error Report Page Class  
 {0cbb503a-f2b2-4b38-8cbc-895cec57db03} Adhoc Ics Finish Page Class  
 {0CE7A4A6-03E8-4A60-9D15-282EF32EE7DA}  
 {0CF774D0-F077-11D1-B1BC-00C04F86C324} HTML Host Encode Object  
 {0CF774D1-F077-11D1-B1BC-00C04F86C324} ASP Host Encode Object  
 {0CFDD070-581A-11D2-9EE6-006008039E37} Generate Black Video  
 {0D0E47ED-7220-411f-8F81-1118095DA5E7} Publication Services Change Data  
 {0D41EBA2-17EA-4B0D-9172-DBD2AE0CC97A} SrDrvWuHelper Class  
 {0D43FE01-F093-11CF-8940-00A0C9054228} FileSystem Object  
 {0D45D530-764B-11d0-A1CA-00AA00C16E65}  
 {0D6417E3-866C-4959-9816-4BF5B85CDAD7} MsasrUI Class  
 {0d81ea0d-13bf-44b2-af1c-fcdf6be7927c} Microsoft DocProp Custom Draw Progress  
 Control  
 {0da7bfdf-c0a0-44eb-be82-b7a82c4721de} ARP CBS Uninstaller Proxy  
 {0DAD2FDD-5FD7-11D3-8F50-00C04F7971E2} Microsoft ATSC Network Provider  
 {0DED49D5-A8B7-4D5D-97A1-12B0C195874D} IBDA\_PinControl  
 {0DF44EAA-FF21-4412-828E-260A8728E7F1} Taskbar and Start Menu  
 {0E2988ED-1DCB-44D0-B9E0-C3AE1D25BE8A} WlanDlg Suppress Autoplay Class  
 {0E5AAE11-A475-4c5b-AB00-C66DE400274E} Shell File System Folder  
 {0E5CBF21-D15F-11D0-8301-00AA005B4383} &Links  
 {0e6daa63-dd4e-47ce-bf9d-fdb72ece4a0d} Device Center Print Context Menu Extension  
 {0EEA25CC-4362-4a12-850B-86EE61B0D3EB} Microsoft DocProp Inplace Droplist Combo  
 Control  
 {0ef801bb-24e7-4059-aeb0-d8727eeaf04c} Mobile Broadband Auto Connect Settings  
 Page Class  
 {0F3F9F91-C838-415E-A4F3-3E828CA445E0} FaxDocument Class  
 {0F424AB8-3D71-3F74-B230-EFB0144788ED}  
 {0f87369f-a4e5-4cfc-bd3e-73e6154572dd} TaskScheduler class  
 {0fb40f0d-1021-4022-8da0-aab0588dfc8b} UPnPAutomationProxy  
 {0FC988D4-C935-4b97-A973-46282EA175C8} PSFactoryBuffer  
 {101A8FB9-F1B9-11d1-9A56-00C04FA309D4} CLSID\_MessageStore  
 {104846ab-42b1-4e38-a80d-136f78c3f258} Browser Progress Aggregator

## SOFTWARE OUTPUT

{10E2414A-EC59-49D2-BC51-5ADD2C36FEBC}	PSFactoryBuffer
{10FEF81C-0DAA-4af0-B714-1F1689C08C8C}	DXVA Allocator
{1108BE51-F58A-4CDA-BB99-7A0227D11D5E}	Microsoft WBEM _IWmiCallSec Call Security
Factory	
{11103421-354C-4CCA-A7A3-1AFF9A5B6701}	MP3 ACM Wrapper MFT
{1138506a-b949-46a7-b6c0-ee26499fdeaf}	WUAppElevator class
{114F5598-0B22-40A0-86A1-C83EA495ADBD}	
{116F8D13-101E-4fa5-84D4-FF8279381935}	CompoundCondition Class
{11993195-1244-4840-AB44-480975C4FFE4}	CFileIo
{11d162b6-1cea-4b4a-8037-2518ecd6554b}	CLSID_FTItemContainer
{11dbb47c-a525-400b-9e80-a54615a090c0}	CLSID_ExecuteFolder
{1202DB60-1DAC-42C5-AED5-1ABDD432248E}	Sync Center Client
{120CED89-3BF4-4173-A132-3CB406CF3231}	DirectSoundParamEqDMO
{122EC645-CD7E-44D8-B186-2C8C20C3B50F}	
{12367cf8-6222-4b34-8ca8-3ce703999e28}	Share Command Execution
{12426E70-50E2-3129-B617-E252B36ECE89}	
{1249B20C-5DD0-44FE-B0B3-8F92C8E6D080}	
{12518493-00B2-11d2-9FA5-9E3420524153}	Mounted Volume
{1277B60F-34D5-48D1-B7BB-59BCA9BC71A8}	Microsoft MPEG-2 Multiplexer Encoder
Property Page	
{1299CF18-C4F5-4B6A-BB0F-2299F0398E27}	PSFactoryBuffer
{12C21EA7-2EB8-4B55-9249-AC243DA8C666}	Virtual Factory for DiagCpl
{12D51199-0DB5-46FE-A120-47A3D7D937CC}	DVD: Pluggable Protocol
{12DA6D0B-021F-4d79-8794-64145F503CA5}	EAP Quarantine Enforcement Client Callback
Component	
{12fc5e89-5446-4a7c-ba46-207a29e2945d}	HomeGroup Confirm Page
{1334e551-b2db-429b-a94a-7d6a226ffcbf}	
{13482EC3-06A3-4bb3-84A9-193302B8DD54}	
{13639463-00DB-4646-803D-528026140D88}	UpdateCollection Class
{13709620-C279-11CE-A49E-444553540000}	Shell Automation Service
{1372A97E-2034-41ee-A6C1-1B68FAFA75A1}	CLSID_ICommunityTransport
{137f5ec6-cf6b-482f-acea-c687dfbd199d}	Microsoft Input Personalization Plug-in
{139D8403-E74F-41d2-B103-8790C5C7A517}	
{13a4bbe8-6527-40cb-a996-1602829541ef}	Frame Automation Object
{13B37A2A-546B-47BF-BBCA-8AC97F1EBDCB}	CMpeg2DataControl
{13D3C4B8-B179-4ebb-BF62-F704173E7448}	CLSID_ContactReadingPane
{13DE4A42-8D21-4C8E-BF9C-8F69CB068FCA}	E-Ink
{14010e02-bbbd-41f0-88e3-eda371216584}	CLSID_SearchFolderItemFactory
{14074e0b-7216-4862-96e6-53cada442a56}	Library Icon Extract Extension
{1438E821-B6D2-11D0-8D86-00C04FD6202B}	CLSID_ApprenticeAcctMgr
{1443904b-34e4-40f6-b30f-6beb81267b80}	cicero sapi layer speech ui server
{14795a8f-78f3-47bd-acb6-e767414fe293}	Shell Apply Properties Undo Unit
{147A9C5D-36F4-4e3e-BD47-F5F207425085}	HomeGroup Printing Listener Class
{14ce31dc-abc2-484c-b061-cf3416aed8ff}	Authentication UI Shutdown Choices
{14D4CBD9-7490-4F25-BAA6-1C5E22F6B1E3}	PimcManager Class
{14d7a407-396b-44b3-be85-5199a0f0f80a}	Media Foundation DShow Source Resolver
{14DD9A1C-7CFF-41be-B1B9-BA1AC6ECB571}	MF AudCap Source Plug-in
{1510FB87-5676-40B9-A227-5D0B66866F81}	PSFactoryBuffer



## SOFTWARE OUTPUT

```

{1531d583-8375-4d3f-b5fb-d23bbd169f22} Windows TXT Previewer
{15756be1-a4ad-449c-b576-df3df0e068d3} Microsoft DocProp Hyperlink Control
{15b0bb4c-0f7d-11D1-b21f-00C04Fb9473f}
{15D6504A-5494-499C-886C-973C9E53B9F1} BDA Tuning Model DVB Tune Request
{15eae92e-f17a-4431-9f28-805e482dafd4} Install New Programs
{15FD01A3-6E5D-4ECD-9EBD-1813CB3887A1} PSFactoryBuffer
{163FDC20-2ABC-11d0-88F0-00A024AB2DBB}
{1643E180-90F5-11CE-97D5-00AA0055595A} Color Space Converter
{1649b154-c794-497a-9b03-f3f0121302f3} PortableDeviceServiceFTM Class
{1649d1cf-deaf-4a68-abe8-5c9f68572fd1} ExecuteAssociation
{16671E5F-0CE6-4CC4-9768-E89FE5018ADE}
{167c0a56-c490-4623-9225-8ffdc546e56c} Top view restore default command
invocation
{1698790a-e2b4-11d0-b0b1-00c04fd8dca6}
{169A0691-8DF9-11d1-A1C4-00C04FD75D13} In-pane search
{16C2C29D-0E5F-45f3-A445-03E03F587B7D} .group shell context menu
{16CA4E03-FE69-4705-BD41-5B7DFC0C95F3} PSFactoryBuffer
{1767B93A-B021-44EA-920F-863C11F4F768}
{176961ec-fbfb-4288-b418-c80c86947481} CVPNDiagHelper Object
{176D323D-E591-4535-9A09-26F698E5AC5D} UserLexiconManager Class
{176d6597-26d3-11d1-b350-080036a75b03} ICM Scanner Management
{17CCA71B-ECD7-11D0-B908-00A0C9223196} Generic WDM Filter Proxy
{17D6CCD8-3B7B-11D2-B9E0-00C04FD8DBF7} DsObjectPicker
{17FC1A80-140E-4290-A64F-4A29A951A867} OpenMediaSharing
{1821B62A-B2A5-4e0a-98C5-9FA0D5BAAAEC} WMPDMCPlaylistsManager Class
{182C40F0-32E4-11D0-818B-00A0C9231C29} COM+ Catalog Server
{1860E246-E924-4F73-B2C5-93E0577E3AA1} IWMiCoreServices Class
{187463A0-5BB7-11D3-ACBE-0080C75E246E} WM ASF Reader
{18907f3b-9afb-4f87-b764-f9a4e16a21b8} CLSID_ConditionAttribute
{1890B385-5DD3-33B4-84DB-24FD1685F33D}
{18C628EE-962A-11D2-8D08-00A0C9441E20} Xml2Dex Class
{190BA3F6-0205-4f46-B589-95C6822899D2} MemoryDiagnosticCustomHandler
{19352205-42B0-4690-9AA4-D7DB9AE5F259} Publication Services Change Data
{193B4137-0480-11D1-97DA-00C04FB9618A} Microsoft DTC Transaction Unmarshaller
(private, internal)
{19603261-6059-43DF-B9E1-8B4352825A90} scanprofileui class
{196f128d-dce9-4090-b061-3d29c6ca32c2} Work Offline or Online
{19b9dcc7-6f37-4dc7-9da6-8af601c5fce2} Mobile Broadband Media Manager
{19BA17F2-2602-4E77-9027-103894607626} Share Media Settings Writer
{1A0391BF-9564-4294-B0A4-06C298929EF9} Share Specific Users
{1A1F4206-0688-4E7F-BE03-D82EC69DF9A5} Sync Center Control
{1A34F5C1-4A5A-46DC-B644-1F4567E7A676}
{1A39680C-2376-4E8E-B168-2148D7FF9AF4}
{1A3F11DC-B514-4B17-8C5F-2154513852F1}
{1A56451B-1315-4012-861E-8587333DD631} WMEnc Screen Capture Filter
{1A8766A0-62CE-11CF-A5D6-28DB04C10000} WDM Streaming Standard Interface Handler
{1ab4a8c0-6a0b-11d2-ad49-00c04fa31a86}
{1AB78400-B5A3-4D91-8ACE-33FCD1499BE6}

```

## SOFTWARE OUTPUT

```

{1AF81E4E-FC45-48ee-B236-A2A663494390} Out Of Proc Mapi Handler
{1B1CAD8C-2DAB-11D2-B604-00104B703EFD} Microsoft WBEM (non)Standard Marshaling
for IEnumWbemClassObject
{1B544C20-FD0B-11CE-8C63-00AA0044B51E} AVI Splitter
{1B544C24-FD0B-11CE-8C63-00AA0044B520} DirectX Transform Wrapper Property Page
{1B7D4AD0-A1B1-43A8-9A46-FB36AB4C1868} WMPDMCDevice Class
{1BA21EC2-FC80-4515-AAAB-F5766A4B88BC} ConfigUI Class
{1BA783C1-2A30-4ad3-B928-A9A46C604C28} Create New Link
{1BB05961-5FBF-11D2-A521-44DF07C10000} XML Graphbuilder
{1BE1F766-5536-11D1-B726-00C04FB926AF} EventSystemTier2
{1BE49F30-0E1B-11D3-9D8E-00C04F72D980} BDA Tuning Model Language Component Type
Class (Broadcast Substream Type)
{1BF18D30-223C-4E0F-9074-C78C1256FD43} Windows Media Player
WMEncAdvancedStreamEdit Class
{1C15D484-911D-11D2-B632-00C04F79498E} Legacy Analog TV Tuner Device Segment
{1c1800c1-3258-44c2-be80-3deadb6c5e39} CLSID_KindDescriptionFactory
{1C5221CB-C1F6-4999-8936-501C2023E4CD} Bluetooth FD Provider
{1C621200-67B2-11D2-9EEB-006008039E37} Black Generator Property Page
{1C82EAD9-508E-11D1-8DCF-00C04FB951F9} Windows Mail Mime Editor
{1cedc5da-3614-11d2-bf96-00c04fd8d5b0}
{1D2680C9-0E2A-469d-B787-065558BC7D43} Fusion Cache
{1d2b8d89-9324-46a0-b797-5725d8c8d881} SdBackupConfig Class
{1D3529C7-671A-468d-AD2A-499A96B073D1} AutoConfig Helper Class
{1D583ABC-8A0E-4657-9982-A380CA58FB4B}
{1d8a9b47-3a28-4ce2-8a4b-bd34e45bceeb} UPnPDescriptionDocument Class
{1DA08500-9EDC-11CF-BC10-00AA00AC74F6} VGA 16 color ditherer
{1DB68FCC-3C8C-49DB-8C76-9A89DE76B8CF} WMPDMCDevicesManager Class
{1DCB3A00-33ED-11D3-8470-00C04F79DBC0} PSFactoryBuffer
{1DF7D126-4050-47F0-A7CF-4C4CA9241333} BDA Tuning Model DVB Satellite Locator
{1E1714A3-50B9-480b-A94A-636D9A9B56D1} Shell Indexer Admin Object
{1E4CEC13-76BD-4ce2-8372-711CB6F10FD1} XML Paper Specification Filter
{1E5300BE-0762-4527-8140-C0FF22DDFC56} Parental Controls Override
{1E589E9D-8A8D-46d9-A2F9-E6D4F8161EE9} MF MPEG Property Handler
{1E651CC0-B199-11D0-8212-00C04FC32C45} Memory Allocator
{1E8F0D70-7399-41BF-8598-7949A2DEC898} Microsoft DocProp Boolean Control
{1ea1ea14-48f4-4054-ad1a-e8aee10ac805} Resizer DMO
{1ea5fb56-9ee8-47dc-8998-f45585c2e3e0} MFPlay Class Factory
{1EC2DE53-75CC-11d2-9775-00A0C9B4D50C} Microsoft Common Language Runtime Meta
Data
{1eeb5b5a-06fb-4732-96b3-975c0194eb39} Itemsview
{1f01f4e9-8b75-4e20-8eb0-e49f17f2be61} Mobile Broadband PromptPinPage Class
{1F0BC6AD-46D4-488B-BE1F-047FC7505E60} ActualWbemAdministrativeLocator Class
{1f1f4e1a-2252-4063-84bb-eee75f8856d5} WM Speech Encoder DMO
{1F247DC0-902E-11D0-A80C-00A0C906241A} Content Index ISearch Creator Object
{1f26a602-2b5c-4b63-b8e8-9ea5c1a7dc2e} SBE2MediaTypeProfile
{1f2e5c40-9550-11ce-99d2-00aa006e086c} Security Shell Extension
{1f3427c8-5c10-4210-aa03-2ee45287d668} User Pinned
{1f3d8aa5-9ebf-4ee4-85c2-ea40379aede8} CScriptedDiag

```

## SOFTWARE OUTPUT

{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Memory Mapped Cache Mgr  
 {1F7D1BE9-7A50-40b6-A605-C4F3696F49C0} ThirdPartyEapDispatcherPeerConfig  
 {1f849cce-2546-4b9f-b03e-4004781bdc40} CLSID\_ExplorerLauncher  
 {1F87137D-0E7C-44d5-8C73-4EFFB68962F2} Microsoft WMI Provider Subsystem Secured

Host

{1FA9085F-25A2-489B-85D4-86326EEDCD87} Manage Wireless Networks  
 {1FCE6123-B675-4790-A629-F3E8AC06F839}  
 {20076C7E-4851-41ed-9EB8-F4E5F2BB0286} PSFactoryBuffer  
 {203b1eed-db9f-40fb-87bd-1990982017d2} WMSDK NamespaceFactory Class  
 {204810b9-73b2-11d4-bf42-00b0d0118b56} UPnPRegistrar  
 {2048EEE6-7FA2-11D0-9E6A-00A0C9138C29} Microsoft OLE DB Row Position Library  
 {2087c2f4-2cef-4953-a8ab-66779b670495} WinHttpRequest Component version 5.1  
 {208D2C60-3AEA-1069-A2D7-08002B30309D} Network  
 {20b1cb23-6968-4eb9-b7d4-a66d00d07cee} Folder View Host  
 {20E25881-F081-448e-85C9-4707A9400593} User Profile WMI Provider  
 {21167137-B7E3-40B6-8863-8386E8C05716} XWizard Factory Generated Class  
 {212690FB-83E5-4526-8FD7-74478B7939CD} Microsoft DTV-DVD Video Decoder  
 {215B77BA-853F-48C4-8DC4-024E0D68A812} SBE Stats - sender side  
 {216C62DF-6D7F-4E9A-8571-05F14EDB766A} Microsoft DVBT Network Provider  
 {217FC9C0-3AEA-1069-A2DB-08002B30309D} Shell Copy Hook  
 {21B22460-3AEA-1069-A2DC-08002B30309D} File Property Page Extension  
 {21EC2020-3AEA-1069-A2DD-08002B30309D} All Control Panel Items  
 {2206CDB0-19C1-11D1-89E0-00C04FD7A829} MSDAINITIALIZE Class  
 {2206CDB2-19C1-11D1-89E0-00C04FD7A829} Microsoft OLE DB Service Component Data

Links

{2206CDB3-19C1-11D1-89E0-00C04FD7A829} MSDASC Error Lookup  
 {220898A1-E3F3-46B4-96EA-B0855DC968B6} Play music command  
 {2227A280-3AEA-1069-A2DE-08002B30309D} Printers  
 {223E7283-D39D-40d9-9BE9-AA61A39FBC5E} Unsecured Net Connect Page Class  
 {228136B0-8BD3-11D0-B4EF-00A0C9138CA4} Catalog Class  
 {228136B8-8BD3-11D0-B4EF-00A0C9138CA4} Cellset Class  
 {22877a6d-37a1-461a-91b0-dbda5aaebc99} Recent Places Folder  
 {2291478C-5EE3-4bef-AB5D-B5FF2CF58352} MSVidCtl SBE Source to iTV Composition

Segment

{22c6c651-f6ea-46be-bc83-54e83314c67f} Folder Infotip  
 {22D6F312-B0F6-11D0-94AB-0080C74C7E95} Windows Media Player  
 {22D8B4F2-F577-4adb-A335-C2AE88416FAB} PSFactoryBuffer  
 {22e5fca2-9c7c-4239-8aed-4d0623f532d8} CMigrationPlugin Object  
 {22EE26E5-2289-11d2-8F43-00C04FC2E0C7}  
 {22ff30d1-a59e-4580-9190-da3042ceca64} Mobile Broadband Roaming Page Class  
 {232b501c-348c-457e-972c-7c3adb1552c1} Config Backup AutoPlay Handler Class  
 {233664b0-0367-11cf-abc4-02608c9e7553} ADs Namespaces Object  
 {233A9694-667E-11d1-9DFB-006097D50408} Windows Mail Address Book  
 {23613363-0028-431D-A49E-A3CD482D3926} Start Menu Group PolicyFilter  
 {236C9559-ADCE-4736-BF72-BAB34E392196}  
 {23CF860E-9D2C-451A-8E83-C79C848D85A6} PSFactoryBuffer  
 {242025BB-8546-48B6-B9B0-F4406C54ACFC} InkSettings Class  
 {24264891-E80B-4fd3-B7CE-4FF2FAE8931F} PSFactoryBuffer

## SOFTWARE OUTPUT

```

{24400D16-5754-11d2-8218-00C04FB687DA} Index Cleaner Prop Bag
{24D568C5-F3AE-4F91-9CD9-AA18876DA7C2} Homegroup Control Panel
{24DC3975-09BF-4231-8655-3EE71F43837D} Video Mixing Renderer 9 Device Segment
{25150040-b8f1-418e-af61-b51071ac1ee2} IEnumExplorerCommand Object On Menu
{25585dc7-4da0-438d-ad04-e42c8d2d64b9} Client application shell extension
{2559a1f0-21d7-11d4-bdaf-00c04f60b9f0} Search
{2559a1f1-21d7-11d4-bdaf-00c04f60b9f0} Help and Support
{2559a1f2-21d7-11d4-bdaf-00c04f60b9f0} Windows Security
{2559a1f3-21d7-11d4-bdaf-00c04f60b9f0} Run...
{2559a1f5-21d7-11d4-bdaf-00c04f60b9f0} E-mail
{2559a1f7-21d7-11d4-bdaf-00c04f60b9f0} Set Program Access and Defaults
{25ab468c-3974-4075-be50-193135461727} Show/hide menu bar command invocation
{25BAAD81-3560-11D3-8471-00C04F79DBC0} MediaDevMgr Class
{25BE9228-00AF-11D2-BF87-00C04FD8D5B0}
{25CBB996-92ED-457e-B28C-4774084BD562} GenericProvider
{25E609E0-B259-11CF-BFC7-444553540000} Microsoft DirectInput
{25E609E1-B259-11CF-BFC7-444553540000} Microsoft DirectInputDevice
{25E609E4-B259-11CF-BFC7-444553540000} Microsoft DirectInput8
{25E609E5-B259-11CF-BFC7-444553540000} Microsoft DirectInput8
{26671179-2ec2-42bf-93d3-64108589cad5} ShellItemArray Shell Namespace helper
{266EEE40-6C63-11cf-8A03-00AA006ECB65} WDM TV Tuner
{266EEE41-6C63-11cf-8A03-00AA006ECB65} TV Tuner Property Page
{267cf8a9-f4e3-41e6-95b1-af881be130ff} Location Folder
{267DB0B3-55E3-4902-949B-DF8F5CEC0191} Custom Composition Segment from WebDVD
Device Segment to Standard Video Renderer Device Segment
{26EC0B63-AA90-458A-8DF4-5659F2C8A18A} BDA Tuning Model Digital Cable Tune
Request
{26EE0668-A00A-44D7-9371-BEB064C98683} Control Panel
{26fdc864-be88-46e7-9235-032d8ea5162e} Merged Folder
{271C3902-6095-4c45-A22F-20091816EE9E} MPEG4 Byte Stream Handler
{273eb5e7-88b0-4843-bfef-e2c81d43aae5} Application Startup Link
{275C23E2-3747-11D0-9FEA-00AA003F8646} Multi Language Support
{2764BCE5-CC39-11D2-B639-00C04F79498E} Generic Graph Composition Segment
{2769280B-5108-498c-9C7F-A51239B63147} PSFactoryBuffer
{276FBFC1-D71F-4619-A7C1-0181077EE283} Microsoft.Windows.Diagnosis.ManagedHost
{2781761E-28E0-4109-99FE-B9D127C57AFE} Windows Defender IOfficeAntiVirus
implementation
{27949969-876A-41D7-9447-568F6A35A4DC}
{280A3020-86CF-11D1-ABE6-00A0C905F375} AC3 Parser Filter
{288a2d5f-253c-46b4-b58c-2ced3180b993} CMI IInstaller
{289228DE-A31E-11D1-A19C-0000F875B132} ListPad class
{28953661-0231-41DB-8986-21FF4388EE9B} MSVidCtl Analog Capture to Encoder
Composition Segment
{289978AC-A101-4341-A817-21EBA7FD046D} Sync Center Conflict Folder
{28AB0005-E845-4FFA-AA9B-F4665236141C} Analog Audio Component Type
{28AF2E16-0190-44F4-9CED-08AF91145361} RA Helper Class
{291EE2A7-BFA5-4e9e-A358-C93655556A6C} VideoProcAmp2 Class
{2933BF90-7B36-11D2-B20E-00C04F983E60} XML DOM Document

```

## SOFTWARE OUTPUT

{2933BF91-7B36-11D2-B20E-00C04F983E60} Free Threaded XML DOM Document  
 {2933BF94-7B36-11D2-B20E-00C04F983E60} XSL Template  
 {2965e715-eb66-4719-b53f-1672673bbefa} Results Folder  
 {2981c306-09ea-405d-9d0f-83337827bd35}  
 {29B5828C-CAB9-11D2-B35C-00105A1F8177} Microsoft WBEM (non)Standard Marshaling  
 for IwbemUnboundObjectSink  
 {29F06F0C-FB7F-44A5-83CD-D41705D5C525} NCPProvider Class  
 {2A005C11-A5DE-11CF-9E66-00AA00A3F464} PropGroupManagerObject Class  
 {2a11bae2-fe6e-4249-864b-9e9ed6e8dbc2} Mpeg4s Decoder DMO  
 {2A11F42C-3E81-4ad4-9CBE-45579D89671A} CivicAddressReportFactory Class  
 {2A196062-812A-4249-B04A-797971DC466C} XML Paper Specification Filter Persistent  
 Handler  
 {2A2699C5-775A-42e9-BF4A-A36FE41BA4CB} TCPIProp Class  
 {2A614240-A4C5-4C33-BD87-1BC709331639} Bidi Spooler APIs  
 {2A6F3A80-5976-11D2-9524-0060081840BC} Silence  
 {2A744BD8-158A-4bbf-9513-4A656F6C01D7} Windows Desktop Search Scope Manager  
 {2af6bcaa-f526-4803-aeb8-5777ce386647} EapMschapv2Cfg Class  
 {2B20FE1A-1B2C-4DC5-8595-616B0E182FD1} MSASR Locale Handler Class (1036)  
 {2B362208-CB07-4fa5-8076-8DB4AA890561} WMPDMCServer Class  
 {2B4B0612-E1F4-376F-A9B9-86BA3F72A670}  
 {2BD40F38-DE45-429D-9D04-24F7C24C78FD} PSFactoryBuffer  
 {2C256447-3F0D-4CBB-9D12-575BB20CDA0A} FaultrepElevatedDataCollection  
 {2C2CEA16-CC79-4C01-B3CE-B5B7CE47101F} Microsoft IME IME Pad interface  
 {2C63E4EB-4CEA-41B8-919C-E947EA19A77C} BDA Tuning Model MPEG2 Tune Request  
 Factory  
 {2C673043-FC2E-4d67-8920-517D24DEBD2C}  
 {2C676B7B-796E-4C59-8209-4D0473E32A17} WMEncSourceSink  
 {2C731933-62A6-31A0-AFE1-1034F46361D2}  
 {2C875213-FCE5-11d1-A0B0-00C04FA31A86}  
 {2CA8CA52-3C3F-11D2-B73D-00C04FB6BD3D} AudioInputMixer Property Page  
 {2D11CF10-4FE0-45B2-88DF-6FFBF92BE9AB} WaitDialog  
 {2D1F634B-BA35-4BA0-A3B4-B03AC5FE724A} DUN Device Center Context Menu Handler  
 {2D2E24CB-0CD5-458F-86EA-3E6FA22C8E64} VMR Allocator Presenter 9  
 {2d3468c1-36a7-43b6-ac24-d3f02fd9607a} A collection of IUnknown objects that can  
 be enumerated  
 {2DB47AE5-CF39-43C2-B4D6-0CD8D90946F4} StreamBufferSink  
 {2DB5E62B-0D67-495F-8F9D-C2F0188647AC}  
 {2DD80115-AD1E-41F6-A219-A4F4B583D1F9} PSFactoryBuffer  
 {2DEA658F-54C1-4227-AF9B-260AB5FC3543} Microsoft PlaySoundService Class  
 {2E095DD0-AF56-47e4-A099-EAC038DECC24} AnalogCable Class  
 {2e167ea7-85e3-4395-995a-77af9875d79a}  
 {2E17C0EF-2851-459b-A3C8-27A41D4BC9F7} Windows Theme Manager API  
 {2e5e84e9-4049-4244-b728-2d24227157c7} UPnPRemoteEndpointInfo  
 {2e7583c7-7eba-4a1a-8468-d03d28477e6f} Shell settings migration  
 {2E9E59C0-B437-4981-A647-9C34B9B90891} Sync Setup Folder  
 {2EBDEE67-3505-43f8-9946-EA44ABC8E5B0} PSFactoryBuffer  
 {2ED326ED-C4C0-434a-B4CE-FB0318D725A7} PSFactoryBuffer  
 {2eeb4adf-4578-4d10-bca7-bb955f56320a} WMAudio Decoder DMO

## SOFTWARE OUTPUT

{2EEEE04-0908-4cdb-AF8F-AC5B768A34C9} Drm Scheme Handler  
 {2F2165FF-2C2D-4612-87B2-CC8E5002EF4C} Advanced Indexing Options Dialog Object  
 {2f2dc38b-34d2-462c-add4-f74cc15510a1} SuggestPopup  
 {2F94D7B0-BF63-11D1-A6A2-00C04FB9988E} EndpointsTable Class  
 {2FB21955-33A2-46A0-8F60-B475DC33FD5A} PSFactoryBuffer  
 {2FE9B39E-0062-41E5-A842-518E212C2CE0} PSFactoryBuffer  
 {301056D0-6DFF-11D2-9EEB-006008039E37} MJPEG Decompressor  
 {3037B4CD-A40B-401B-B676-2017EE8FAFF4} Wordpad DOCX Filter  
 {30766BD2-EA1C-4F28-BF27-0B44E2F68DB7} Windows Search Root  
 {3080F90D-D7AD-11D9-BD98-0000947B0257} Show Desktop  
 {3080F90E-D7AD-11D9-BD98-0000947B0257} Window Switcher  
 {30d49246-d217-465f-b00b-ac9ddd652eb7} Identity Store  
 {3124C396-FB13-4836-A6AD-1317F1713688} SAX XML Reader 3.0  
 {3140F5B6-093F-4F94-9141-5DF9EE10BC27} MSASR Locale Handler Class (1033)  
 {31430c59-bed1-11D1-8De8-00C04FC2E0C7} InstallationAgent Class  
 {317E92FC-1679-46FD-A0B5-F08914DD8623} text persistent handler for mapi email  
 {317F3AA1-A5F5-4310-9401-BAE5DAC386C6} Layer Composer  
 {31879719-E751-4DF8-981D-68DFF67704ED} Sync Command State Handler  
 {31b11d80-9ed7-44f7-b1cd-c95992a738b9} TcpiObj Class  
 {31b231f6-546d-4f9b-ac95-0f963d72559c} Favorites  
 {31DCBC0C-20D8-40b0-A409-F4474A942358} Windows Photo Viewer Gallery Interface  
 {323CA680-C24D-4099-B94D-446DD2D7249E} For &People...  
 {32557D3B-69DC-4F95-836E-F5972B2F6159} LayoutFolder  
 {32624F4B-F1D5-4877-989E-555640109D2B} MSSCP Class  
 {32714800-2E5F-11d0-8B85-00AA0044F941} PSFactoryBuffer  
 {3283EEBF-E67D-31AC-8481-A968F3A77E9A} Microsoft AAC Audio Decoder MFT  
 {328B0346-7EAF-4BBE-A479-7CB88A095F5B} Script Encoder Object  
 {32BAED44-34B5-11D3-9315-00C04F72D6CF} InfraProfileExistsErrorPage  
 {32C5A81F-27C0-4E66-A894-786F646F1236} ClassicW Class  
 {32d186a7-218f-4c75-8876-dd77273a8999} BDA Data Services Feature Segment  
 {32DA2B15-CFED-11D1-B747-00C04FC2B085} ADs DN With String Object  
 {32E7DC13-1E22-4D7E-8AC7-D2E718DE8042} MPEG-I Stream Splitter  
 {3336B8BF-45AF-429f-85CB-8C435FBF21E4} Browser Application State  
 {334125C0-77E5-11D3-B653-00C04F79498E} PSFactoryBuffer  
 {334857cc-f934-11d2-ba96-00c04fb6d0d1} TF\_InputProcessorProfiles  
 {336475D0-942A-11CE-A870-00AA002FEAB5} Onex PLAP Smartcard Credential Provider  
 {33BCC8EC-0D01-4E10-AD3D-4DAF749873ED} ACM Class Manager  
 {33C4643C-7811-46FA-A89A-768597BD7223} WaveIn Class Manager  
 {33C53A50-F456-4884-B049-85FD643ECFED} SAMI (CC) Reader  
 {33c86cd6-705f-4ba1-9adb-67070b837775} WpcNotificationsMigration  
 {33D9A760-90C8-11D0-BD43-00A0C911CE86} WlanBalloonHandler Class  
 {33D9A761-90C8-11d0-BD43-00A0C911CE86} Windows Live Services Class  
 {33D9A762-90C8-11d0-BD43-00A0C911CE86}  
 {33de48c4-943f-4b96-8cd8-b117c94576cf}  
 {33FACFE0-A9BE-11D0-A520-00A0D10129C0}  
 {343D770D-7788-47c2-B62A-B7C4CED925CB}  
 {348C9CFF-CB90-4024-AE22-F17259A3934B}  
 {34A19196-274E-4D75-9D30-D7A45A0A4178}

## SOFTWARE OUTPUT

{34c219bd-85c1-4338-95e8-788a36901dc2} Configure Windows Portable Device Task Class

{3508C064-B94E-420b-A821-20C8096FAADC} AtscPspParser Class

{35117bca-71f9-4399-8709-f380c7aaa8bd} Screen Fade

{35298344-96A6-45E7-9B6B-62ECC6E09920} PSFactoryBuffer

{3529B1D2-313A-4202-BD3E-5996B7E18A10}

{352EC2B7-8B9A-11D1-B8AE-006008059382} Shell Application Manager

{3540D440-5B1D-49cb-821A-E84B8CF065A7} MSVidCtl Analog Capture to XDS Composition

Segment

{354F7156-A4F6-47F5-A028-FE2000E92132} PSFactoryBuffer

{355DFFAA-3B9F-435c-B428-5D44290BC5F2} WpcSettingsProvider Class

{356F2F88-05A6-4728-B9A4-1BFBCE04D838}

{35786D3C-B075-49b9-88DD-029876E11C01} Portable Devices

{35C61CC2-5851-4F2D-89B6-4F9BB4B4193F} Microsoft Search Property System Change

Notify Handler

{3692CA39-E082-4350-9E1F-3704CB083CD5}

{3697790B-223B-484E-9925-C4869218F17A}

{36eef7db-88ad-4e81-ad49-0e313f0c35f8} Windows Update

{36f0bd14-d84d-468c-b79c-9990f3fa897f} Multi Object Elevation Factory

{370A1D5D-DDEB-418C-81CD-189E0D4FA443} VBI Codec

{372FCE38-4324-11D0-8810-00A0C903B83C} CertConfig Class

{3730bbf8-631a-48fb-9085-e2143c11563b} XWizard Factory Generated Class (HomeGroup

Empty Hook Page)

{3734FF83-6764-44B7-A1B9-55F56183CDB0} Sync Center (Internal)

{373984C9-B845-449B-91E7-45AC83036ADE} XML Schema Cache

{3756e7f5-e514-4776-a32b-eb24bc1efe7a} State of built-in commands

{375ff002-dd27-11d9-8f9c-0002b3988e81} WCN-Config Function Discovery Provider

Class

{37734C4D-FFA8-4139-9AAC-60FBE55BF3DF} BlbEngine Class

{379E501F-B231-11D1-ADC1-00805FC752D8} MsxmlIsland

{37A61C8B-7F8E-4d08-B12B-248D73E9AB4F} Secure Http Scheme Handler

{37B0353C-A4C8-11D2-B634-00C04F79498E} File Playback Device Segment

{37B03543-A4C8-11D2-B634-00C04F79498E} Standard Video Renderer Device Segment

{37B03544-A4C8-11D2-B634-00C04F79498E} Standard Audio Renderer Device Segment

{37de7045-5056-456f-8409-c871e0f8b0e0} Trun Gateway Protocol Class

{37E92A92-D9AA-11D2-BF84-8EF2B1555AED} Audio Renderer Advanced Properties

{37ea3a21-7493-4208-a011-7f9ea79ce9f5} Open Containing Folder Menu

{37efd44d-ef8d-41b1-940d-96973a50e9e0} Windows Sidebar Properties

{380BA9E8-E1E6-33C3-8CA9-385FA6E48C88}

{381DDA3C-9CE9-4834-A23E-1F98F8FC52BE}

{384ea5ae-ade1-4e8a-8a9b-7bea78fff1e9} CLSID\_BinaryAutoList

{3882134d-14cf-4220-9cb4-435f86d83f60} PortableDeviceValuesCollection Class

{389EA17B-5078-4CDE-B6EF-25C15175C751}

{38A98528-6CBF-4CA9-8DC0-B1E1D10F7B1B}

{38F03426-E83B-4E68-B65B-DCAE73304838} Custom Composition Segment from Data

Services to Time Shift Sink

{3901CC3F-84B5-4FA4-BA35-AA8172B8A09B} DirectSound 8.0 Object

{3908C3CD-4478-4536-AF2F-10C25D4EF89A} WiaVideo Class

## SOFTWARE OUTPUT

```

{39981129-C287-11D0-8D8C-00C04FD6202B} CLSID_CMAPIAcctImport
{39AE2AEA-D4D5-4DA0-AE47-C020E1BE4BE5} CLSID_JetDatabaseSession
{39F8D76B-0928-11D1-97DF-00C04FB9618A} Microsoft DTC Transaction
{3A614B00-FB18-46F3-950E-682A46A48B9F} PSFactoryBuffer
{3A8CCBCB-0EFD-43a3-B838-F38A552BA237} CTocEntryList
{3A9428A7-31A4-45E9-9EFB-E055BF7BB3DB} BDA Tuning Model Channel ID Tune Request
{3ABEAF4C-F48F-4517-A9B0-8AD6A94A99A1} Publication Services Data
{3ad05575-8857-4850-9277-11b85bdb8e09} Copy/Move/Rename/Delete/Link Object
{3ADCE5CC-13C8-4573-B328-ED438EB694F9} CaviTocParser
{3AE86B20-7BE8-11D1-ABE6-00A0C905F375} MPEG-2 Splitter
{3B881B82-5BF4-4657-A3A2-CCE17E4FD39A} Nap Server Info class
{3bb4118f-ddfd-4d30-a348-9fb5d6bf1afe} Time Categorizer
{3BBE95A4-C53F-11d1-B3A2-00A0C9083365} TRUN Tx Begin Class
{3BBE95DA-C53F-11d1-B3A2-00A0C9083365} Trun Gateway Tx Class
{3BBE95F5-C53F-11d1-B3A2-00A0C9083365} Trun Gateway Tx Crash Recovery Class
{3BBE95FB-C53F-11d1-B3A2-00A0C9083365} Trun Gateway Instance Class
{3BBE95FE-C53F-11d1-B3A2-00A0C9083365} Trun Gateway Instance Scan Class
{3c2654c6-7372-4f6b-b310-55d6128f49d2} Alphabetical Categorizer
{3C305196-50DB-11D3-9CFE-00C04FD930C5} DirectDraw7 Object
{3C3A70A7-A468-49B9-8ADA-28E11FCCAD5D} RASrv Class
{3C4708DC-B181-46A8-8DA8-4AB0371758CD} MSVidCtl SBE Source to Video Mixing
Renderer Composition Segment
{3C5F432A-EF40-4669-9974-9671D4FC2E12} MMC Plugable Internet Protocol
{3CCF8A41-5C85-11d0-9796-00AA00B90ADF} Shell DeskBarApp
{3CE74DE4-53D3-4D74-8B83-431B3828BA53} TF_DisplayAttributeMgr
{3D07A539-35CA-447C-9B05-8D85CE924F9E} Closed Captions Analysis Filter
{3D112E22-62B2-11D1-9FEF-00600832DB4A} MMCTask class
{3d154a2d-d911-437e-a30c-5f56a9b7081d} Extract Const Icon Handler
{3D813DFE-6C91-4A4E-8F41-04346A841D9C} MXXMLWriter 3.0
{3D96ED94-5D75-4165-9E1F-1A642C7BA316} Windows Media Player WMEncTextInputSource
Class
{3dad6c5d-2167-4cae-9914-f99e41c12cfa} Include In Library Sub Context Menu
{3dd6bec0-8193-4ffe-ae25-e08e39ea4063} NPPProvider
{3DD82D10-E6F1-11D2-B139-00105A1F77A1} WMI instrumentation:
Win32_PowerManagementEvent
{3E000D72-A845-4CD9-BD83-80C07C3B881F} CMLUAUTIL
{3E458037-0CA6-41aa-A594-2AA6C02D709B} SBE2FileScan
{3E4D4F1C-2AEE-11D1-9D3D-00C04FC30DF6} oleprn Class
{3E5FC7F9-9A51-4367-9063-A120244FBEC7} CMSTPLUA
{3E784A01-F3AE-4DC0-9354-9526B9370EBA} SAXAttributes 3.0
{3EE60F5C-9BAD-4CD8-8E21-AD2D001D06EB} InkObject Class
{3eef301f-b596-4c0b-bd92-013beafce793} Destkop Undo Manager
{3EF76D68-8661-4843-8B8F-C37163D8C9CE} Custom Composition Segment from CCA to
Stream Buffer Source
{3F281000-E95A-11d2-886B-00C04F869F04} Com Call Wrapper Unmarshal Class
{3F35F070-99D6-11D2-8D10-00A0C9441E20} Audio Repackager
{3f454f0e-42ae-4d7c-8ea3-328250d6e272} Automation context menu
{3F6953F0-5359-47FC-BD99-9F2CB95A62FD} Personal Start Menu

```



## SOFTWARE OUTPUT

{3f6bc534-dfa1-4ab4-ae54-ef25a74e0107} System Restore  
 {3FC0B520-68A9-11D0-8D77-00C04FD70822} Display Control Panel HTML Extensions  
 {3FF292B6-B204-11CF-8D23-00AA005FFE58} FoxOLEDB 1.0 Object  
 {3FF566F0-6E6B-49D4-96E6-B78886692C62}  
 {3FFB3B8C-EB99-472b-8902-E1C1B05F07CF} LPCM Byte Stream Handler  
 {4003191F-71FF-49A2-B591-05C606FADB8B} WMPPlayer MusicPropPage Class  
 {40419485-C444-4567-851A-2DD7BFA1684D} Phone and Modem Control Panel  
 {404A6DE5-D4D6-4260-9BC7-5A6CBD882432}  
 {40C3D757-D6E4-4b49-BB41-0E5BBEA28817} Video Media Properties Handler  
 {40dd6e20-7c17-11ce-a804-00aa003ca9f6} Shell extensions for sharing  
 {41070793-59E4-479A-A1F7-954ADC2EF5FC}  
 {4125dd96-e03a-4103-8f70-e0597d803b9c} Microsoft Attachment Services  
 {41457294-644C-4298-A28A-BD69F2C0CF3B} ASF Byte Stream Handler  
 {417BAB8B-9D22-4A88-9DA0-98C4AB6745D5} WPD Settings Commit Page Class  
 {418008F3-CF67-4668-9628-10DC52BE1D08} BDA Tuning Model MPEG2 Component Type  
 Class (Broadcast Substream Type)  
 {418AFB70-F8B8-11CE-AAC6-0020AF0B99A3} Quality Management Property Page  
 {418c8b64-5463-461d-88e0-75e2afa3c6fa} Explorer Browser Results Folder  
 {41937347-2aba-4d4c-a4ca-6fe4f11f1bac} Network Item Factory  
 {41B23C28-488E-4E5C-ACE2-BB0BBABE99E8} HHCtrl Object  
 {41B9BE05-B3AF-460C-BF0B-2CDD44A093B1} XML filter  
 {41E300E0-78B6-11ce-849B-444553540000} Display Effects CPL Extension  
 {42044394-8c34-11d1-83bc-00c04fbbc34e}  
 {42150CD9-CA9A-4EA5-9939-30EE037F6E74} Microsoft MPEG-2 Video Encoder  
 {424bed78-ef88-4b7c-945c-b8cf46d56e20} Authentication UI Last Logged On Username  
 {427BC7E3-F833-4584-8745-CFAB9D7A5761} CTaskConditionCombiner  
 {427FD3D4-F30A-4033-84EF-CBB1A955D9F7} AggregateAssociationList  
 {42aedc87-2188-41fd-b9a3-0c966feabec1} MruPidlList  
 {42C9B9F5-16FC-47ef-AF22-DA05F7C842E3} WAV Byte Stream Handler  
 {42DFB618-A403-4401-908F-FE979B2215C8} PSFactoryBuffer  
 {43136EB5-D36C-11CF-ADBC-00AA00A80033} NodeInit 1.0 Object  
 {4315D437-5B8C-11D0-BD3B-00A0C911CE86} DeviceMoniker  
 {43232233-8338-4658-ae01-0b4ae830b6b0} PortableDeviceDispatchFactory Class  
 {43324B33-A78F-480F-9111-9638AACCC832}  
 {4336a54d-038b-4685-ab02-99bb52d3fb8b} Public Folder  
 {435899C9-44AB-11D1-AF00-080036234103} DSPrintQueue Class  
 {437ff9c0-a07f-4fa0-af80-84b6c6440a16} Command Folder  
 {43B07326-AAE0-4B62-A83D-5FD768B7353C} InkRectangle Class  
 {43FB1553-AD74-4ee8-88E4-3E6DAAC915DB} InkCollector Class  
 {4405b37b-60fe-49ed-ba8f-691a78f84daf}  
 {44121072-A222-48f2-A58A-6D9AD51EBBE9}  
 {443E7B79-DE31-11D2-B340-00104BCC4B4A} WbemUnauthenticatedLocator Class  
 {4444AC9E-242E-471B-A3C7-45DCD46352BC} VMR Allocator Presenter DDXcl Mode  
 {44CB442B-9DA9-49df-B3FD-023777B16E50} Http Scheme Handler  
 {44da8435-b187-4dd6-8f32-9341eb7e4c3c} CLSID\_CSmapiProxy  
 {44EC053A-400F-11D0-9DCD-00A0C90391D3} Registrar Class  
 {44f3dab6-4392-4186-bb7b-6282ccb7a9f6} MyDocuments menu and properties  
 {44F9A03B-A3EC-4F3B-9364-08E0007F21DF} TaskSymbol Class

## SOFTWARE OUTPUT

{4522c772-9a2b-4920-ad7f-62d3d15eac52} Restore Default Favorite Links Command  
 {45597c98-80f6-4549-84ff-752cf55e2d29} Add to Windows Media Player list  
 {455ACF57-5345-11D2-99CF-00C04F797BC9} PSFactoryBuffer  
 {455f6102-c83a-4d07-ba36-b6da9d589ae2} RdpAudioSink Class  
 {45670FA8-ED97-4F44-BC93-305082590BFB} Microsoft XPS Shell Metadata Handler  
 {4582746F-473B-4022-A7E9-887CBEDD8F85} SBE IO counters  
 {4582eba9-6aa1-4d79-824e-728929ef455d} XWizard Factory Generated Class  
 {4590F811-1D3A-11D0-891F-00AA004B2E24} WBEM Locator  
 {4590F812-1D3A-11D0-891F-00AA004B2E24} Microsoft WBEM WbemClassObject Marshalling  
 proxy  
 {461CDD3F-D54E-4033-A0AA-6CD24F152AA1} WlanDlg Get Key UI Page Class  
 {4657278A-411B-11d2-839A-00C04FD918D0} Shell Drag and Drop helper  
 {4662DAB0-D393-11D0-9A56-00C04FB68B66}  
 {46763EE0-CAB2-11CE-8C20-00AA0051E5D4} Obsolete Font  
 {469afbdF-084f-4dc9-904f-9e824c48bc37} Folder Initialization Handler  
 {46C0A7DC-928A-485a-959F-1F9EF8686A11}  
 {46C166AA-3108-11D4-9348-00C04F8EEB71} Home Networking Configuration Manager  
 {47135eea-06b6-4452-8787-4a187c64a47e} SdrRestoreService Class  
 {47354492-827E-4b8a-B318-C80EBA1381F0} CClusterDetectorEx  
 {4753da60-5b71-11cf-b035-00aa006e0975} ADs Provider Object  
 {477EC299-1421-4bdd-971F-7CCB933F21AD} File Scheme Handler  
 {47D4D946-62E8-11cf-93BC-444553540000} DirectSound Object  
 {48025243-2D39-11CE-875D-00608CB78066} Internal Text Renderer  
 {480FF4B0-28B2-11D1-BEF7-00C04FBF8FEF} DirectMusicCollection  
 {48123bc4-99d9-11d1-a6b3-00c04fd91555} XML Document  
 {48527bb3-e8de-450b-8910-8c4099cb8624} Empty Recycle Bin verb invocation  
 {489331DC-F5E0-4528-9FDA-45331BF4A571} CInitiateWinSAT Class  
 {48e2ed0f-98c2-4a37-bed5-166312ddd83f} MFReadWrite Class Factory  
 {48e7caab-b918-4e58-a94d-505519c795dc} Start Menu Folder  
 {49010C18-B110-421a-9047-ADCA421CBC40} IMRequestRA Class  
 {49638B91-48AB-48B7-A47A-7D0E75A08EDE} BDA Tuning Model Analog Locator  
 {498B0949-BBE9-4072-98BE-6CCAEB79DC6F} SmartRenderEngine Class  
 {4991d34b-80a1-4291-83b6-3328366b9097} Background Intelligent Transfer Control  
 Class 1.0  
 {499EAEEA-2737-4849-8BB6-47F107EAF358} CTocParser  
 {49ACAA99-F009-4524-9D2A-D751C9A38F60} PSFactoryBuffer  
 {49B2791A-B1AE-4C90-9B8E-E860BA07F889} MMC Application Class  
 {49BD2028-1523-11D1-AD79-00C04FD8FDFF} Microsoft WBEM Unsecured Apartment  
 {49C407EF-78B9-4C82-A40B-2FE02F8E771D} Windows Theme Thumbnail Preview  
 {49eb6558-c09c-46dc-8668-1f848c290d0b} Scope Picking Dialog  
 {49f171dd-b51a-40d3-9a6c-52d674cc729d} UIAutomationCrossBitnessHook64 Class  
 {49F371E1-8C5C-4d9c-9A3B-54A6827F513C} Sharing Configuration Manager  
 {4a04656d-52aa-49de-8a09-cb178760e748} Recycle Bin Manager  
 {4A16043F-676D-11d2-994E-00C04FA309D4} CLSID\_DatabaseSession  
 {4A1E5ACD-A108-4100-9E26-D2FAFA1BA486} IGD Property Page  
 {4A2286E0-7BEF-11CE-9BD9-0000E202599C} MPEG Audio Codec  
 {4A38E4EF-F55B-4A59-8F02-BDEFB0B1308A} CGNPMpeg2DataControl  
 {4A4EBE8E-AE27-4AA3-B702-F365C4A90FAC} PSFactoryBuffer

## SOFTWARE OUTPUT

```

{4A56AF32-C21F-11DB-96FA-005056C00008}
{4A5869CF-929D-4040-AE03-FCAFC5B9CD42} Generic Sink Segment
{4A65D267-1539-4BD1-921D-1C49B3E58EB7} SnapInFailureReporter
{4A6B8BAD-9872-4525-A812-71A52367DC17} RasGcw LUA
{4a714c8e-e664-4024-9c74-1a82a3da842a} Authentication UI Background
{4a76b469-7b66-4dd4-ba2d-ddf244c766dc} GSM ACM Wrapper MFT
{4a7ded0a-ad25-11d0-98a8-0800361b1103} MyFolder menu and properties
{4AF3F4A4-06C8-4B79-A523-633CC65CE297} WBEM Disk Quota Volume Provider
{4AF4A5FC-912A-11D1-B945-00A0C90312E1} Microsoft Docking Bar Property Bag
{4B181F0F-48C8-4e80-A2AF-E3099AAC069B} PresentationHost in-proc handler
{4B2E958D-0393-11D1-B1AB-00AA00BA3258} COM+ Active Process Iteration Server
{4B534112-3AF6-4697-A77C-D62CE9B9E7CF} Sync Center Event Properties Extension
{4B59AFCC-B8C3-408A-B670-89E5FAB6FDA7}
{4b6657e4-b973-46cd-9bb3-6e5ebd82448f} PortableDeviceWMDRM Class
{4B966436-6781-4906-8035-9AF94B32C3F7} SPP Class
{4BDD6232-2E55-4A1F-AAAD-961D76F439BA} PSFactoryBuffer
{4bec2015-bfa1-42fa-9c0c-59431bbe880e} Shell URL
{4C4A5E40-732C-11D0-8816-00A0C903B83C} CertServerPolicy Class
{4C596AEC-8544-4082-BA9F-EB0A7D8E65C6} CivicAddress Report Class
{4c649c49-c48f-4222-9a0d-cbbf4231221d} Photo Printing with Templates Wizard
{4c892621-6757-4fe0-ad8c-a6301be7fba2} Windows Settings Page
{4cadfae1-5512-456a-9d65-5b5e7e9ca9a3} PortableDeviceClassExtension Class
{4CB43D7F-7EEE-4906-8698-60DA1C38F2FE} UpdateSession Class
{4CFC7932-0F9D-4BEF-9C32-8EA2A6B56FCB} Microsoft WMI Provider Subsystem Decoupled
Registrar
{4D111E08-CBF7-4f12-A926-2C7920AF52FC} Shell Security Editor
{4D317113-C6EC-406A-9C61-20E891BC37F7} RASettingProperty Class
{4D73E9D0-4716-3585-BE8B-7FF800EE5866}
{4DB1AD10-3391-11D2-9A33-00C04FA36145} PSFactoryBuffer
{4DD1D1C3-B36A-4eb4-AAEF-815891A58A30} Vector Class
{4DD441AD-526D-4A77-9F1B-9841ED802FB0} SAXAttributes
{4DDA1941-77A0-4fb1-A518-E2185041D70C} CTocGeneratorDmo
{4DE225BF-CF59-4CFC-85F7-68B90F185355} Microsoft WMI Provider Subsystem
{4df0c730-df9d-4ae3-9153-aa6b82e9795a} Known Folder Manager
{4DF929E7-4C5E-4587-A598-7ED7B3D6E462} AddMdmObj Class
{4E14FBA2-2E22-11D1-9964-00C04FBBB345} Event System
{4E40F770-369C-11d0-8922-00A024AB2DBB} Security Shell Extension
{4ea9a1b7-e521-4813-a9f8-ba6484902cb5} SMB Helper Class
{4EFE2452-168A-11d1-BC76-00C04FB9453B} MidiOut Class Manager
{4F4DB904-CA35-4A3A-90AF-C9D8BE7532AC} RecoExt Class
{4F58F63F-244B-4c07-B29F-210BE59BE9B4} .group shell extension handler
{4F664F91-FF01-11D0-8AED-00C04FD7B597} OleSNMP Class
{4F695794-BFCF-48B0-A323-F874F9BD45F2} Windows Media Player
WMEncFileTransferSource Class
{4FA18276-912A-11D1-AD9B-00C04FD8FDFF} InProcWbemLevel1Login Class
{4FAF64F1-A3BA-4172-B922-E6A22ACF7E3D} XWizard Factory Generated Class
{4FD2A832-86C8-11D0-8FCA-00C04FD9189D}
{4FDEF69C-DBC9-454e-9910-B34F3C64B510} PSFactoryBuffer

```

## SOFTWARE OUTPUT

```

{4FE24495-28CE-4920-A4C4-E556E1F0DF2A} CToc
{4FF2FE0E-E74A-4B71-98C4-AB7DC16707BA}
{50040C1D-BDBF-4924-B873-F14D6C5BFD66} MediaDevMgrClassFactory Class
{5058292D-A244-4840-AB44-480975C4FFE4} CTocCollection
{5068B32E-DFE0-48C2-9816-4549033447DB} PSFactoryBuffer
{506D89AE-909A-44F7-9444-ABD575896E35} DxtAlphaSetter Class
{5088B39A-29B4-4d9d-8245-4EE289222F66} QueryParserManager Class
{50B1904B-F28F-4574-93F4-0BADE82C69E9}
{50cc2c18-b48c-4764-8f3f-0331ed295ce4} Undo command invocation
{50D42F09-ECD1-4B41-B65D-DA1FDAA75663}
{510C4E33-05D5-438B-9852-E8406EFF033D} PSFactoryBuffer
{51372af3-cae7-11cf-be81-00aa00a2fa25} MTSPackage
{51653423-E62D-4FF7-894A-DABB2B8E21E2} CrawlStartPages Task Handler
{517F6AA6-D6FA-46D0-8094-17FF17E4CCF4} HomeGroup Security Hosted Listener
{51B4ABF3-748F-4E3B-A276-C828330E926A} Video Mixing Renderer 9
{5210f8e4-b0bb-47c3-a8d9-7b2282cc79ed} WMAPro over S/PDIF DMO
{522e34a4-07f7-40a1-94d0-1bfe832efc3a} PSFactoryBuffer
{524B13ED-2E57-40B8-B801-5FA35122EB5C} DrawAttrs Class
{5255EFED-103A-4444-B124-F88F99E4EF8D} HomeGroup Printer Hosted Listener
{527c9a9b-b9a2-44b0-84f9-f0dc11c2bcfb} Microsoft DocProp Static Property Control
{52968B13-8F33-33DB-B55F-ED57D7D05E8A}
{529A9E6B-6587-4F23-AB9E-9C7D683E3C50} TF_ThreadMgr
{52A2AAAE-085D-4187-97EA-8C30DB990436} HHCtrl Object
{52ce2fe5-04c3-42fd-8a8b-4251affb8408} CLSID_ResultSetManager
{52CFFDFE-A115-4164-AFB1-EAD719C52C15} Biometrics Policy object
{52e4e90a-f4af-460a-9e60-fdfb86c9dd5d} Windows Media Player WMEncoder Class
{52F15C89-5A17-48e1-BBCD-46A3F89C7CC2} LeafCondition Class
{52FD5C49-A63D-45EC-8687-98DA8B7BFE6A} video clips pix command support
{5323BCB5-0431-42be-A482-5EE76F243A28}
{5326dddc-ec38-428d-b219-ce6dad35de3} Connect to a network
{53362C64-A296-4F2D-A2F8-FD984D08340B} RemoteProxyFactory32 Class
{53445BED-3213-453B-A12A-79AA20A702DC} LegacyPrintUI Class
{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0} Control Panel command object for Start
menu and desktop
{53a01e9d-61cc-4cb0-83b1-31bc8df63156} Microsoft DocProp Icon List Control
{53bd6b4e-3780-4693-afc3-7161c2f3ee9c} MruLongList
{53BEDF0B-4E5B-4183-8DC9-B844344FA104} MAPI Mail Previewer
{53C74826-AB99-4d33-ACA4-3117F51D3788}
{5408B2F0-C816-11D1-8F99-00600895E7D5} Interface Proxy Stub
{545AE700-50BF-11D1-9FE9-00600832DB4A} MMCCtrl class
{548968f5-17f7-4751-a581-ff0f1c732995} Authentication UI System Settings
{5491AB67-AFEB-48B1-B8DF-B2D63810EF40} PSFactoryBuffer
{549365d0-ec26-11cf-8310-00aa00b505db} ADsDSOobject
{54A05253-96FA-4B98-B8FD-9534D7255914} PSFactoryBuffer
{54D8502C-527D-43F7-A506-A9DA075E229C}
System.Management.Instrumentation.ManagedCommonProvider
{550DDA30-0541-11D2-9CA9-0060B0EC3D39} XML Data Source Object
{5537E283-B1E7-4EF8-9C6E-7AB0AFE5056D} CRasProvider

```

## SOFTWARE OUTPUT

{555F3418-D99E-4E51-800A-6E89CFD8B1D7} HwDeviceCustomProperties  
 {5569e7f5-424b-4b93-89ca-79d17924689a} Windows Media Player Plug-in Registrar  
 {559C6BAD-1EA8-4963-A087-8A6810F9218B} CThumbnailGeneratorDmo  
 {55B3A0BD-4D28-42fe-8CFB-FA3EDFF969B8}  
 {55d7b852-f6d1-42f2-aa75-8728a1b2d264} Size Categorizer  
 {56198675-BD59-3B10-8346-583781462CEF}  
 {563DC062-B09A-11D2-A24D-00104BD35090} WSHController  
 {566296fe-e0e8-475f-ba9c-a31ad31620b1}  
 {566A2EFF-5651-4020-AC1A-EB48E4571EA3} Windows Media SDK HTTP Source Plugin  
 {5686a0d9-fe39-409f-9dff-3fdbcb849f9f5} Mpeg4s Decoder MFT  
 {56ad4c5d-b908-4f85-8ff1-7940c29b3bcf} Window Property Store  
 {56FDF344-FD6D-11d0-958A-006097C9A090} Task Bar Communication  
 {573bdf38-df23-427f-äcb8-a67abd702698} VssModuleKeeper  
 {5740A302-EF0B-45ce-BF3B-4470A14A8980} iTV Capture Feature Segment  
 {57558531-C262-471E-95DB-8B181925C61B} Infrastructure Setup Page Class  
 {57635537-C856-4cc2-AE5C-62C34708070C} Shell Security Zone Checker  
 {57651662-CE3E-11D0-8D77-00C04FC99D61} CmdFileIcon  
 {576C9E85-1300-4EF5-BF6B-D00509F4EDCD} Sync Center Handler Properties Extension  
 {577FAA18-4518-445E-8F70-1473F8CF4BA4} Utility Object for Binding Events  
 SubObjects in Script Variables  
 {57C06EAA-8784-11D0-83D4-00A0C911E5DF} Microsoft Client Configuration Notify  
 Object  
 {57f8510b-a5e2-41da-a8f0-8a5ae85dffffd} Browser Class Factory Creator  
 {5805137A-E348-4F7C-B3CC-6DB9965A0599}  
 {5815ADD9-95C5-44F2-8262-3BCD56AA3147} Windows Search Manager Event Sink  
 {58221C65-EA27-11CF-ADCF-00AA00A80033} FILEMGMT 1.0 Object  
 {58221C66-EA27-11CF-ADCF-00AA00A80033} SvcVwr 1.0 Object  
 {58221C69-EA27-11CF-ADCF-00AA00A80033} FILEMGMT 1.0 Object  
 {58221C6A-EA27-11CF-ADCF-00AA00A80033} SvcVwr 1.0 Object  
 {5839FCA9-774D-42A1-ACDA-D6A79037F57F} Microsoft WBEM \_WbemFetchRefresherMgr  
 Proxy Helper  
 {58476F97-6464-4e49-9BCB-DD88816A60A3}  
 {5848A73D-E9C2-499E-BB92-887CABCB2BD6} Microsoft XPS Active Document  
 {58859c43-2c82-454b-86c0-9efb11e54838} Ratings Categorizer  
 {58AB2366-D597-11d1-B90E-00C04FC9B263} EapTlsCfg Class  
 {58C2B4D0-46E7-11D1-89AC-00A0C9054129} DirectMusicSynth  
 {58E3C745-D971-4081-9034-86E34B30836A} Speech Recognition  
 {58ECEE30-E715-11CF-B0E3-00AA003F000F} FoxOLEDB 1.0 Object  
 {58fb76b9-ac85-4e55-ac04-427593b1d060} Certificate Services Client Task Handler  
 {59031a47-3f72-44a7-89c5-5595fe6b30ee} UsersFiles  
 {59099400-57FF-11CE-BD94-0020AF85B590} Disk Copy Extension  
 {591209c7-767b-42b2-9fba-44ee4615f2c7} Application Registration  
 {59347292-B72D-41F2-98C5-E9ACA1B247A2} FaxCommon Class  
 {593817A0-7DB3-11CF-A2DE-00AA00B93356} DirectDraw Clipper Object  
 {596742A5-1393-4e13-8765-AE1DF71ACAFB} Microsoft Breadcrumb Bar  
 {59699770-2BF1-46C6-857C-1D509DB7079E} GlobalServiceDS Class  
 {597D4FB0-47FD-4aff-89B9-C6CFAE8CF08E} ManipulationProcessor Class  
 {599F9021-5643-4965-9949-E88975EFFF0E} PSFactoryBuffer

## SOFTWARE OUTPUT

{59A437AB-74F3-4de2-AFE6-54203634C4DD} Share Permission List  
 {59CE6880-ACF8-11CF-B56E-0080C7C4B68A} Performance Property Page  
 {59DC47A8-116C-11D3-9D8E-00C04F72D980} BDA Tuning Model Component Class(Broadcast Substream)  
 {5A41EFA3-6C01-43DC-8C49-110151B36C70} Line 21 Decoder Text Output  
 {5A580C11-E5EB-11d1-A86E-0000F8084F96} CLSID\_IHTTPMailTransport  
 {5B035261-40F9-11D1-AAEC-00805FC1270E} Network Configuration Component Object  
 {5B18AB61-091D-11D1-97DF-00C04FB9618A} Microsoft DTC Transaction Manager  
 {5b4dae26-b807-11d0-9815-00c04fd91972} Menu Band  
 {5b53b2c2-46d6-433e-ab6e-b82efef22b6e} ExplorerCommandEnumerator  
 {5b858418-cfb4-4b32-8501-54d8b0c59f90} Item Enumerator Over Categories  
 {5BAF654A-5A07-4264-A255-9FF54C7151E7} UpdateDownloader Class  
 {5BF9AA75-D7FF-4aee-AA2C-96810586456D}  
 {5C140836-43DE-11d3-847D-00C04F79DBC0} SCPTRANS Class  
 {5C5C1935-0235-4434-80BC-251BC1EC39C6}  
 {5C63C1AD-3956-4FF8-8486-40034758315B} Home Networking Sharing Configuration Manager  
 {5cb66670-d3d4-11cf-acab-00a024a55aef} COM+ Extended Transaction Context Component  
 {5CDCB131-A1A1-4FE9-9A10-80EFFE042AE0} video clips container  
 {5D08B586-343A-11D0-AD46-00C04FD8FDFF} Microsoft WBEM Event Subsystem  
 {5d1026ee-3f2e-4ccb-a83d-cefb7ac22a71} Share Media Control Panel  
 {5d4d54b3-9fb4-4662-8173-c48568d5e79e} Percent Categorizer  
 {5D6179C8-17EC-11D1-9AA9-00C04FD8FE93} Microsoft Local Users and Groups MMC Snap-in  
 {5D6179D2-17EC-11D1-9AA9-00C04FD8FE93} Microsoft Local Users and Groups MMC Snap-in About Provider  
 {5D8E73F7-4989-4ac8-8A98-39BA0D325302} MSVidCtl Digital TV to iTV Composition Segment  
 {5D9DD151-65F4-11CE-900D-00AA00445589} Microsoft DTC Transaction Manager Proxy (private, internal)  
 {5DB2625A-54DF-11D0-B6C4-0800091AA605} ICM Monitor Management  
 {5DC41690-C6A6-11d1-9D35-006008B0E5CA}  
 {5DC41691-C6A6-11d1-9D35-006008B0E5CA}  
 {5DC41692-C6A6-11d1-9D35-006008B0E5CA}  
 {5DC41693-C6A6-11d1-9D35-006008B0E5CA}  
 {5DC41694-C6A6-11d1-9D35-006008B0E5CA}  
 {5E032150-8C1E-4c9e-BC60-36E9BFFCFF56} HomeGroup Peer Manager  
 {5E1395B2-B685-44e3-8AED-E2304D85ACD1} WiaWow64  
 {5E33D52F-2EE2-48EE-80FC-543DFF43E326} IGD Helper Class  
 {5E6AB780-7743-11CF-A12B-00AA004AE837} Microsoft Internet Toolbar  
 {5e941d80-bf96-11cd-b579-08002b30bfeb} Plain Text persistent handler  
 {5ead82c2-28f1-4f7f-956d-d37420b5a687} Mobile Broadband Connecting Page Class  
 {5ef4af3a-f726-11d0-b8a2-00c04fc309a4} Recycle Bin Cleaner  
 {5f4baad0-4d59-4fcd-b213-783ce7a92f22} WIA Event Prompt Class  
 {5F5295E0-429F-1069-A2E2-08002B30309D} Drive Property Page Extension  
 {5F5AFF4A-2F7F-4279-88C2-CD88EB39D144} Microsoft MPEG-2 Encoder  
 {5FA29220-36A1-40F9-89C6-F4B384B7642E} Shell Message Handler

## SOFTWARE OUTPUT

```

{6004c347-d3f3-472a-8f9e-319b5c583d55} DESC_ItemThumbnail
{60173D16-A550-47f0-A14B-C6F9E4DA0831} Mount Point Rename
{602BDCE5-CA64-4E91-B27C-FFCA48978A00} Windows Search Index Notification Sink
{603D3800-BD81-11d0-A3A5-00C04FD706EC} Background Task Scheduler
{603D3801-BD81-11d0-A3A5-00C04FD706EC} Shared Task Scheduler
{6047F837-D527-467E-9DC1-6D51F92D9E45} Wordpad ODT Filter
{60542247-0249-417D-949B-2F0CC7EE1165} Manual Setup Page Class
{60664caf-af0d-0005-a300-5c7d25ff22a0} Shell Local Machine Object
{60F6E464-4DEF-11d2-B2D9-00C04F8EEC8C} Old Files In Root Prop Bag
{60F6E465-4DEF-11d2-B2D9-00C04F8EEC8C} Temp Files Prop Bag
{60F6E466-4DEF-11d2-B2D9-00C04F8EEC8C} Setup Files Prop Bag
{60F6E467-4DEF-11d2-B2D9-00C04F8EEC8C} Uninstall Prop Bag
{60fd46de-f830-4894-a628-6fa81bc0190d} DropTarget Object for Photo Printing
Wizard
{6131A8EC-78CE-11d2-A3F2-3078302C2030}
{61b68808-8eee-4fd1-acb8-3d804c8db056} Contact class
{61E79517-4A4E-45D8-9219-30E71A9EFF39} TabletButtonExtendedActions Class
{61F7B364-432C-4D04-BBC1-7FC1BF3807A8} Bluetooth Bluewire Shell property
extension object
{61FFC721-B206-45d0-B02E-6AA7E52E1575} DictationHost Class
{62079164-233b-41f8-a80f-f01705f514a8} EVR Graph Optimizer
{62112AA1-EBE4-11cf-A5FB-0020AFE7292D} Shell Automation Folder View
{622a8646-1096-4765-8e07-91a3e661cef9} XWizard Factory Generated Class (HomeGroup
Leave Hook Page)
{622D47B6-CEEC-4DE1-8056-B6D16F29BC97} Microsoft WBEM Rpc Message Sender
{626BAFE6-E5D6-11D1-B1DD-006097D503D9} CLSID_OERulesManager
{6276916E-8F41-35C7-B1D2-1D289A63BE7C}
{6295DF27-35EE-11D1-8707-00C04FD93327} Sync Manager (Legacy)
{6295DF2D-35EE-11D1-8707-00C04FD93327} Sync Center (Private)
{62AE1F9A-126A-11D0-A14B-0800361B1103}
{62BE5D10-60EB-11d0-BD3B-00A0C911CE86} System Device Enumerator
{62CE7E72-4C71-4D20-B15D-452831A87D9D} Microsoft H264 Video Decoder MFT
{6311429E-2F1A-4777-880F-C7289FD10169} Inplace Share Engine
{632A2D3D-86AF-411A-8654-7511B51B3D5F} Lattice Class
{636B9F10-0C7D-11D1-95B2-0020AFDC7421} DirectMusic
{636c15cf-df63-4790-866a-117163d10a46} MFRemoteDesktopPlugin Class
{639F5AF5-BCED-4369-AC34-360B16D955FD} GestureRecognizer Class
{63A865AB-859E-4f15-8AEC-77FC615653D9} WMPPlayer FileFormatPropPage Class
{63B51F81-C868-11D0-999C-00C04FD655E1} Shell Icon Overlay Manager
{63FA5E69-87FE-432d-8F62-9D7A3D7D09C3} WMPPlayer VideoPerfPropPage Class
{6438570B-0C08-4A25-9504-8012BB4D50CF} Tuner Marshaling Helper
{64577982-86D7-11d1-BDFC-00C04FA31009} CLSID_IHashTable
{645FF040-5081-101B-9F08-00AA002F954E} Recycle Bin
{64818D10-4F9B-11CF-86EA-00AA00B929E8}
{64818D11-4F9B-11CF-86EA-00AA00B929E8}
{649c5690-507e-494a-9e89-1eb24e4bce3d} WMPMDE LPCM SINK ACTIVATE
{64B8F404-A4AE-11D1-B7B6-00C04FB926AF} PSFactoryBuffer
{64BC32B5-4EEC-4de7-972D-BD8BD0324537} Search Control

```

## SOFTWARE OUTPUT

```

{64D8A8E0-80A2-11d2-8CF3-00A0C9441E20} RenderEngine Class
{6504AFED-A629-455C-A7F1-04964DEA5CC4} BDA Tuning Model ISDB Satellite Locator
{650503CF-9108-4DDC-A2CE-6C2341E1C582} WebProxy Class
{6522CF99-94C7-4958-B18D-4F6159E6926B} Policy for DWM items tree item callback
object for sysdm.cpl
{65303443-AD66-11D1-9D65-00C04FC30DF6} OleCvt Class
{6543D242-A80B-44A3-B828-95C1EC452423} ActualWbemAuthenticatedLocator Class
{659cdea7-489e-11d9-a9cd-000d56965251} Background Intelligent Transfer Control
Class 3.0
{65BD0711-24D2-4FF7-9324-ED2E5D3ABAFa} MediaDet
{65d00646-cde3-4a88-9163-6769f0f1a97d} InkOverlay Class
{660b90c8-73a9-4b58-8cae-355b7f55341b} Start Menu Cache
{661FF7F6-F4D1-4593-B59D-4C54C1ECE68B} WmiPerf Class Provider
{66275315-bfa5-451b-88b6-e56ebc8d9b58} Library Property Handler
{662C0206-72AD-4ee9-899F-5E1735F60A55} WMPDMCMedia Class
{66742402-F9B9-11D1-A202-0000F81FEDEE}
{66d56b60-97b7-4e6a-9aa1-3ec5e3fdaa0f} Winsock Diagnostic Helper Class
{66e4e4fb-f385-4dd0-8d74-a2efd1bc6178} Shell Image Data Factory
{66EC5C50-45B7-48cd-81D6-20A712011AD1} SpeechUXHost Class
{66eea0f5-001a-4073-a496-783f86fcf4c0} Windows Data Burn
{6705C562-0AE7-40EA-8474-F39DAB1813D0} RAS Media Manager
{6746c347-576b-4f73-9012-cdfeea251bc4} CLSID_ScopeFactory
{674B6698-EE92-11D0-AD71-00C04FD8FDFF} Microsoft WBEM Call Context
{6756A641-DE71-11d0-831B-00AA005B4383} MRU AutoComplete List
{675F097E-4C4D-11D0-B6C1-0800091AA605} ICM Printer Management
{67718415-c450-4f3c-bf8a-b487642dc39b} Windows Features
{6785BFAC-9D2D-4be5-B7E2-59937E8FB80A} Other Users Folder
{67CA7650-96E6-4FDD-BB43-A8E774F73A57} HomeGroup Control Panel
{67F07E00-CCEF-11D2-9EF9-006008039E37} Audio Mixer Property
{681FD532-7EC2-4548-9ECE-44AABCFBD254} Registry Provider Class
{682159d9-c321-47ca-b3f1-30e36b2ec8b9} CLSID_DesktopExplorerHost
{687607A0-6BA1-4355-99F4-4E3D749FFB19} WlanDlgOneXUIPage Class
{687D3367-3644-467a-ADFE-6CD7A85C4A2C} MPEG-2 Demultiplexer(NoClock)
{687e55ca-6621-4c41-b9f1-c0eddc94bb05} SdController Class
{68b07bff-cb50-4d60-a7d5-02b1a523bc8c} SearchConnector Icon Extract Extension
{68B67DA9-7212-396E-9528-33F70547660E}
{68c67565-410e-45e6-8560-4091ae193481}
{68E3F2FD-31AE-4441-BB6A-FD7047525F90}
{68e52c1c-37cb-41d2-afe1-1e77d5f10676} Autoplay Device Event Handler Info
{69127644-2511-4DF5-BC6A-26178254AA40} RemoteAssistance Class
{6935DB93-21E8-4ccc-BEB9-9FE3C77A297A} Custom MRU AutoCompleted List
{693644B0-6858-11D2-9EEB-006008039E37} Still Video Property Page
{69546697-5b53-43c5-8391-9e227b54957b} IARPUinstallerProxy
{698A4FFC-63A3-4E70-8F00-376AD29363FB} Wordpad OOXML Document Filter
{699745C2-5066-4B82-A8E3-D40478DBEC8C}
{69AD4AEE-51BE-439b-A92C-86AE490E8B30} Legacy Background Intelligent Transfer
Control Class
{69B37063-2BB6-43b5-A109-60E69A77840F} WcsPlugInService Class

```



## SOFTWARE OUTPUT

```

{69BE8BB4-D66D-47C8-865A-ED1589433782}
{69F9CB25-25E2-4BE1-AB8F-07AA7CB535E8} Sync Center Isolation Collection (Private)
{6A08CF80-0E18-11CF-A24D-0020AFD79767} ACM Wrapper
{6A205B57-2567-4a2c-B881-F787FAB579A3} Microsoft DocProp Inplace Calendar Control
{6A2A9381-5A92-4296-9397-564673AE1FDD} CLSID_HomeGroupListenerNotify
{6A2E0670-28E4-11D0-A18C-00A0C9118956} IAMVideoControl
{6A68CC80-4337-4dbc-BD27-FBFB1053820B} CSearchLanguageSupport Class
{6AD28EE1-5002-4E71-AAF7-BD077907B1A4} MSVidCtl MPEG2 Decoder to Closed
Captioning Composition Segment
{6AFCCE9E-85F0-475C-944E-9357B84A4975} Infrastructure Error Page Class
{6B13B293-30FD-4abb-8E41-29B1F88297E2} Windows Media Player OCXGeneralPropPage
Class
{6B2D6BA0-9F3E-4f27-920B-313CC426A39E} Open Packaging API Factory Object
{6b33163c-76a5-4b6c-bf21-45de9cd503a1} Shell Publishing Wizard Object
{6B362280-6915-11D2-951F-0060081840BC} Silence Generator Property Page
{6B462062-7CBF-400D-9FDB-813DD10F2778}
{6B6F9D2D-6D49-4026-83A6-86DFC1C3C6F0} INI Property Set Storage Handler
{6B750899-F157-47D7-9C08-257E7A35141D}
{6B831E4F-A50D-45FC-842F-16CE27595359} Storage Processor Default Confirmation UI
{6B9228DA-9C15-419e-856C-19E768A13BDC} Windows Desktop Gadgets
{6BC096B1-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096B3-0CE6-11D1-BAAE-00C04FC2E20D} IAS Pipeline
{6BC096B7-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096B8-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096BC-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096D5-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DA-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DB-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DC-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DD-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DE-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096DF-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E0-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E1-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E2-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E3-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E4-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096E5-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09894-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09896-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09897-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09898-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09899-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989A-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989B-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989C-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989D-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC0989E-0CE6-11D1-BAAE-00C04FC2E20D}

```

## SOFTWARE OUTPUT

```

{6BC0989F-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A4-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A5-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A6-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A7-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A8-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A9-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098AC-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098AD-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC1CFFA-8FC1-4261-AC22-CFB4CC38DB50} Default Video Renderer
{6BF0A714-3C18-430b-8B5D-83B1C234D3DB} PSFactoryBuffer
{6BF52A52-394A-11d3-B153-00C04F79FAA6} Windows Media Player
{6c19be35-7500-11d1-ad94-00c04fd8fdff} Microsoft Wbem Event filter marshaling
proxy
{6C5CFCDA-1F1A-4c9e-8D65-94771169D0B9} GameDetails Class
{6ca50344-051a-4ded-9779-a43305165e35}
{6CF48EF8-44CD-45d2-8832-A16EA016311B}
{6CFAD761-735D-4AA5-8AFC-AF91A7D61EBA} Mpeg-2 Video Stream Analysis
{6d18ad12-bde3-4393-b311-099c346e6df9} Background Intelligent Transfer Control
Class 2.0
{6D3951EB-0B07-4fb8-B703-7C5CEE0DB578} Advanced Indexing Options Dialog Object
{6D5313C0-8C62-11D1-B2CD-006097DF8C11} Folder Options Property Page Extension
{6D75C88D-82A0-3994-A751-3B82F490D22C}
{6D8BB3D3-9D87-4a91-AB56-4F30CFFFE9F} Explorer Search Band
{6d8ff8d2-730d-11d4-bf42-00b0d0118b56} UPnPEventingManager
{6d8ff8dc-730d-11d4-bf42-00b0d0118b56} UPnPDynamicContentSource
{6d8ff8dd-730d-11d4-bf42-00b0d0118b56} UPnPDescriptionManager
{6d8ff8df-730d-11d4-bf42-00b0d0118b56} UPnPDevicePersistenceManager
{6d8ff8e0-730d-11d4-bf42-00b0d0118b56} UPnPContainer
{6d8ff8e1-730d-11d4-bf42-00b0d0118b56} UPnPContainerManager
{6d8ff8e5-730d-11d4-bf42-00b0d0118b56} UPnPValidationManager
{6d8ff8e7-730d-11d4-bf42-00b0d0118b56} UPnPContainerManager64
{6d8ff8e8-730d-11d4-bf42-00b0d0118b56} UPnPContainer64
{6DA736C9-DCDE-4651-82A8-56E4EF1D8DD7} CLSID_ScFileExecute
{6DAF9757-2E37-11D2-AEC9-00C04FB68820} MOF Compiler
{6db29a9b-10d0-4b93-b86a-188fc998eff8} InfraCreateTask
{6DFD7C5C-2451-11d3-A299-00C04F8EF6AF} Folder Options
{6e18f9c6-a3eb-495a-89b7-956482e19f7a} WinSAT Accessibility Object
{6e29fabf-9977-42d1-8d0e-ca7e61ad87e6} UIAutomation Registrar Class
{6e33091c-d2f8-4740-b55e-2e11d1477a2c} Shell Image Recompression Object
{6E3D2E94-E6D8-4afd-AFDE-ABD26CA88BF5} FaultrepDataCollectionInProc
{6E4FCB12-510A-4d40-9304-1DA10AE9147C} InkTablets Class
{6e682784-1eca-4cf2-988d-96b6e89e9a4d} CLSID_SearchIDListFactory
{6E78DAD9-E187-4D6E-BA63-760256D6F405} Microsoft Session And Connection Provider
{6EB22881-8A19-11D0-81B6-00A0C9231C29} Catalog Class
{6EDD6D74-C007-4E75-B76A-E5740995E24C} PSFactoryBuffer
{6EF07F29-F9B8-4DA4-B59E-13DEA060AD60}
{6efeae9e-014c-436a-8aac-35da9535adc0} Windows Media Player InputCollection Class

```

## SOFTWARE OUTPUT

```

{6F26A6CD-967B-47FD-874A-7AED2C9D25A2} Video Port Manager
{6f33340d-8a01-473a-b75f-ded88c8360ce} HomeGroup UI Status
{6f45dc1e-5384-457a-bc13-2cd81b0d28ed} PasswordProvider
{6F74FDC5-E366-11d1-9A4E-00C04FA309D4} CLSID_MessageDatabase
{6F74FDC6-E366-11d1-9A4E-00C04FA309D4} CLSID_FolderDatabase
{6F7C8E8F-DC69-4e3f-BC05-439962A05FD5} CLSID_HomeGroupProvider
{6F8DAE82-43A2-47AA-B0E7-47B7E82F705F} WMEncSourcePluginWrapper
{6FE54E0E-009F-4E3D-A830-EDFA71E1F306} Bluetooth Personal Area Connection
{7007ACC1-3202-11D1-AAD2-00805FC1270E} Dial-up Connection UI Class
{7007ACC3-3202-11D1-AAD2-00805FC1270E} Inbound Connection UI Class
{7007ACC4-3202-11D1-AAD2-00805FC1270E} Internet Connection UI Class
{7007ACC5-3202-11D1-AAD2-00805FC1270E} LAN Connection UI Class
{7007ACC6-3202-11D1-AAD2-00805FC1270E} VPN Connection UI Class
{7007ACC7-3202-11D1-AAD2-00805FC1270E} Network Connections
{7007ACC8-3202-11D1-AAD2-00805FC1270E} Network Connections Enum
{7007ACCF-3202-11D1-AAD2-00805FC1270E} Network Connections Tray
{7007ACD1-3202-11D1-AAD2-00805FC1270E} Network Common Connections Ui
{7007ACD3-3202-11D1-AAD2-00805FC1270E} Net Connections UI Utilities Class
{7007ACD4-3202-11D1-AAD2-00805FC1270E} PPPoE UI Class
{7007ACD5-3202-11D1-AAD2-00805FC1270E} Shared Access Connection UI Class
{7016F8FA-CCDA-11D2-B35C-00105A1F8177} Microsoft WBEM (non)Standard Marshaling
for IWbemMultiTarget
{7071EC01-663B-4bc1-A1FA-B97F3B917C55} Build Connections Options Page Class
{7071EC05-663B-4bc1-A1FA-B97F3B917C55} Display Connection Options Page Class
{7071EC07-663B-4bc1-A1FA-B97F3B917C55} Handle Diagnostics Page Class
{7071EC13-663B-4bc1-A1FA-B97F3B917C55} Connect To Work Connect To Internet Page
Class
{7071EC31-663B-4bc1-A1FA-B97F3B917C55} ISP Offer Page Class
{7071EC32-663B-4bc1-A1FA-B97F3B917C55} ISP Confirm Page Class
{7071EC33-663B-4bc1-A1FA-B97F3B917C55} ISP CD Page Class
{7071EC61-663B-4bc1-A1FA-B97F3B917C55} Display Internet Existing Connections Page
Class
{7071EC62-663B-4bc1-A1FA-B97F3B917C55} Display Work Existing Connections Page
Class
{7071EC71-663B-4bc1-A1FA-B97F3B917C55} Create Dial-up Task Class
{7071EC75-663B-4bc1-A1FA-B97F3B917C55} Create VPN Task Class
{7071EC77-663B-4BC1-A1FA-B97F3B917C55} XWizard Factory Generated Class
{7071ECA0-663B-4bc1-A1FA-B97F3B917C55} Connect To Internet Task Class
{7071ECA3-663B-4bc1-A1FA-B97F3B917C55} Connect To The Internet Detection Hook
Page Class
{7071ECA5-663B-4bc1-A1FA-B97F3B917C55} Connect To The Internet Creation Hook Page
Class
{7071ECA7-663B-4bc1-A1FA-B97F3B917C55} Connect To The Internet Testing Hook Page
Class
{7071ECA8-663B-4bc1-A1FA-B97F3B917C55} Connect To The Internet Hook Page Class
{7071ECA9-663B-4bc1-A1FA-B97F3B917C55} Connect To The Internet Diagnostics Hook
Page Class
{7071ECAF-663B-4bc1-A1FA-B97F3B917C55} Connect To The Internet Finish Page Class

```

## SOFTWARE OUTPUT

```

{7071ECB0-663B-4bc1-A1FA-B97F3B917C55} Connect To Work Task Class
{7071ECB3-663B-4bc1-A1FA-B97F3B917C55} Connect To Work Detection Hook Page Class
{7071ECB4-663B-4bc1-A1FA-B97F3B917C55} Connect To Work Existing Connections Page
Class
{7071ECB5-663B-4bc1-A1FA-B97F3B917C55} Connect To Work Creation Hook Page Class
{7071ECB6-663B-4bc1-A1FA-B97F3B917C55} XWizard Factory Generated Class
{7071ECB7-663B-4bc1-A1FA-B97F3B917C55} Connect To Work Testing Hook Page Class
{7071ECB8-663B-4bc1-A1FA-B97F3B917C55} Connect To Work Hook Page Class
{7071ECBF-663B-4bc1-A1FA-B97F3B917C55} Connect To Work Finish Page Class
{7071ECD0-663B-4bc1-A1FA-B97F3B917C55} Connect To Bluetooth Task Class
{7071ECD5-663B-4bc1-A1FA-B97F3B917C55} Display Bluetooth Adapters Page Class
{7071ECE0-663B-4bc1-A1FA-B97F3B917C55} Connect To Network Task Class
{7071ECE5-663B-4bc1-A1FA-B97F3B917C55} Connect To Network Page Class
{7071ECF1-663B-4bc1-A1FA-B97F3B917C55} Message Page Class
{7071ECFA-663B-4bc1-A1FA-B97F3B917C55} Network Tasks Host Class
{70804ECC-7272-4dc8-AFFC-97CD66AAA282} Windows Desktop Search Map Plugin
{7098BB2E-EB80-4433-BEF6-DF45206A41DC} Vista Share Engine
{709E2729-F883-441e-A877-ED3CEFC975E6} ProfileNotifyHandler Class
{70cba7d2-50a5-4383-8aa5-b378c01c7364} CLSID_LegacyFindFiles
{70E102B0-5556-11CE-97C0-00AA0055595A} Video Renderer
{70f598e9-f4ab-495a-99e2-a7c4d3d89abf} WMAudio Encoder DMO
{70f98452-3c38-4271-8e76-6f444852ebc8} PortableDeviceWiaCompat Class
{70FF37C0-F39A-4B26-AE5E-638EF296D490} RARegSetting Class
{7122A82D-E722-4AFC-AA87-EAA77D8CFCE1} Windows Media Player WMEnc5PointWavSource
Class
{71285C44-1DC0-11D2-B5FB-00104B703EFD} Microsoft WBEM (non)Standard Marshaling
for IWbemObjectSink
{713790EE-5EE1-45ba-8070-A1337D2762FA} WTVFile Thumbnail Handler
{713aacc8-3b71-435c-a3a1-be4e53621ab1} AnimateWindowSize Object
{7165c8ab-af88-42bd-86fd-5310b4285a02} ContactManager class
{717ef4fe-ac8d-11d0-b945-00c04fd8d5b0} DsPropertyPages.User Special Info
{71932D43-3CA5-46EF-B013-3F9A695996ED} DMO Wrapper Filter
{71985F4B-1CA1-11D3-9CC8-00C04F7971E0}
{71D99464-3B6B-475C-B241-E15883207529} Sync Results Folder
{71E32BAA-73EE-40a1-933C-F166F0192B72} Show thumbnails instead of icons tree item
callback object for sysdm.cpl
{71E38F91-7E88-11CF-9EDE-0080C78B7F89} MTxAS Object
{71f96385-ddd6-48d3-a0c1-ae06e8b055fb} Explorer Browser
{71F96460-78F3-11d0-A18C-00A0C9118956} %Filter_XBar%
{71F96461-78F3-11d0-A18C-00A0C9118956} Analog Crossbar Property Page
{71F96462-78F3-11d0-A18C-00A0C9118956} WDM TV Audio
{71F96463-78F3-11d0-A18C-00A0C9118956} TV Audio Property Page
{71F96464-78F3-11D0-A18C-00A0C9118956} VideoProcAmp Property Page
{71F96465-78F3-11D0-A18C-00A0C9118956} CameraControl Property Page
{71F96466-78F3-11D0-A18C-00A0C9118956} VideoDecoder Property Page
{71F96467-78F3-11D0-A18C-00A0C9118956} VideoStreamConfig Property Page
{720D4AC0-7533-11D0-A5D6-28DB04C10000} KsTopologyInfo Class
{722b3793-5367-4446-b6bb-db89b05c1f24} ItemHandlerCache

```

## SOFTWARE OUTPUT

```

{725F645B-EAED-4fc5-B1C5-D9AD0ACCB45E} File Open Dialog Legacy
{728a21c5-3d9e-48d7-9810-864848f0f404} PortableDevice Class
{72A7994A-3092-4054-B6BE-08FF81AEFFFC} Sharing Elevated Virtual Factory
{72b36e70-8700-42d6-a7f7-c9ab3323ee51} Search Connector Folder
{72C24DD5-D70A-438B-8A42-98424B88AFB8} Windows Script Host Shell Object
{72c57034-02c4-4e9f-bf9c-ca711031757e} Shell File Operation Undo Unit
{72C97D74-7C3B-40AE-B77D-ABDB22EBA6FB} StringCollection Class
{72d3edc2-a4c4-11d0-8533-00c04fd8d503} ADs Property Entry Object
{72eb61e0-8672-4303-9175-f2e4c68b2e7c} Namespace Walker
{73647561-0000-0010-8000-00AA00389B71} WDM Streaming Standard Data Type Handler
{73C037E7-E5D9-4954-876A-6DA81D6E5768}
{73D14237-B9DB-4efa-A6DD-84350421FB2F} MSVidCtl Digital TV to CCA Composition
Segment
{73DA5D04-4347-45D3-A9DC-FAE9DDBE558D} CSectionList
{73E709EA-5D93-4B2E-BBB0-99B7938DA9E4} Microsoft WMI Provider Subsystem Host
{740EC24D-46AD-4334-A076-41CCC3F8D9B4} PBDA Class
{74246bfc-4c96-11d0-abef-0020af6b0b7a} Device Manager
{743a6e3b-a5df-43ed-b615-4256add790b8} MFPsiFilter
{7447A267-0015-42C8-A8F1-FB3B94C68361}
{745057c7-f353-4f2d-a7ee-58434477730e} AEC
{745a5add-6a71-47b9-9bb9-31dd3a6913d4} Authentication UI CredUI Helper
{7469AE5E-1CA1-4181-970C-BDFD8EAA2C4F} PSFactoryBuffer
{74807f67-0058-440d-8600-65541a7fbbea} PSFactoryBuffer
{7487cd30-f71a-11d0-9ea7-00805f714772} Background Thumbnail Generator
{75048700-EF1F-11D0-9888-006097DEACF9} ActiveDesktop
{7542E960-79C7-11D1-88F9-0080C7D771BF} Event Subscription
{75847177-f077-4171-bd2c-a6bb2164fbd0} Private Profile Object
{75C9378A-7E89-11d2-B116-00805FC73204}
{75dff2b7-6936-4c06-a8bb-676a7b00b24b} CLSID_SeparateMultipleProcessExplorerHost
{760C4B83-E211-11D2-BF3E-00805FBE84A6} Windows Media Services DRM Storage object
{7669CAD6-BDEC-11D1-A6A0-00C04FB9988E} ProtocolsTable Class
{76765b11-3f95-4af2-ac9d-ea55d8994f1a} Property System Both Class Factory
{76B4FCAC-BB29-11DB-96F1-005056C00008} PBDA ETFilter
{76be8257-c4c0-4d37-90c0-a23372254d27} Indexer Status Update Object
{76D0CB12-7604-4048-B83C-1005C7DDC503}
{76f014ec-1b0c-4a15-a029-4c0fdf12b5b1} Briefcase Storage Object
{7751F46E-39B2-4b50-A7E3-23EF598ECD85} Selector Class
{77597368-7B15-11D0-A0C2-080036AF3F03} PrintUIShellExtension Class
{7763B7C0-A5FD-4AA9-BD1B-58B17137236B} Location Description
{777BA815-2498-4875-933A-3067DE883070} XWizard Task Stub
{777BA816-2498-4875-933A-3067DE883070} XWizard Page Stub
{777BA81A-2498-4875-933A-3067DE883070} XWizard Virtual Factory
{777BA851-2498-4875-933A-3067DE883070} XWizard Type plugin for Win32 Class
{777BA853-2498-4875-933A-3067DE883070} XWizard Type plugin for DUI Class
{777BA87C-2498-4875-933A-3067DE883070} Public XWizard Manager Class
{777BA8D2-2498-4875-933A-3067DE883070} Public Simple Marshal Class
{777BA8E3-2498-4875-933A-3067DE883070} Private XWizard Page Enumeration Manager
Class

```

## SOFTWARE OUTPUT

{777BA8E5-2498-4875-933A-3067DE883070} Private XWizard Task Enumeration Manager  
 Class  
 {777BA8E7-2498-4875-933A-3067DE883070} Private XWizard Host Enumeration Manager  
 Class  
 {777BA8E9-2498-4875-933A-3067DE883070} Private XWizard Registry Information  
 Manager Class  
 {777BA8F5-2498-4875-933A-3067DE883070} Private XWizard Registration Manager Class  
 {777BA8F9-2498-4875-933A-3067DE883070} Private XWizard Factory Registration  
 Manager Class  
 {777BA8FB-2498-4875-933A-3067DE883070} Private XWizard Type Registration Manager  
 Class  
 {777D0CFF-0375-43b9-8532-FB04A4903593} Windows Media Player Effects Activate  
 {77F10CF0-3DB5-4966-B520-B7C54FD35ED6} Custom Destination List  
 {77F419AA-771A-45ff-AC66-7567FA3243D3} SMB Share Engine  
 {77F7F122-20B0-4117-A2FB-059D1FC88256} WPDSERVICEPROVIDER Class  
 {780102B0-C43B-4876-BC7B-5E9BA5C88794} PSFactoryBuffer  
 {78103FB7-AED7-4066-8BCD-30BB27B02331} Microsoft WBEM WMI Object Factory  
 {782fc20a-81cf-43de-a625-072155bcd30c} XWizard Factory Generated Class (HomeGroup  
 Create Hook Page)  
 {784215B4-0D2E-11D3-920A-00C0DF10D434} MediaDetFilter  
 {7849596a-48ea-486e-8937-a2a3009f31a9} PostBootReminder object  
 {78530B75-61F9-11D2-8CAD-00A024580902} MS Timeline  
 {786CDB70-1628-44A0-853C-5D340A499137} TabletManager Class  
 {7886B467-66D4-4163-82BA-D9212FDB4CA8} Windows Security Health Agent Callback  
 Component  
 {7888E5FE-6C66-4A34-B217-FA2292073F4A} PSFactoryBuffer  
 {78F3955E-3B90-4184-BD14-5397C15F1EFC} Performance Information and Tools  
 {78fe669a-186e-4108-96e9-77b586c1332f} Content Index Null Stemmer  
 {79376820-07D0-11CF-A24D-0020AFD79767} DirectSound Audio Renderer  
 {797A9BB1-9E49-4e63-AFE1-1B45B9DC8162} DeviceHostICSSupport Class  
 {798059F0-89CA-4160-B325-AEB48EFE4F9A} CColorControlDmo  
 {7986d495-ce42-4926-8afc-26dfa299cadb} Authentication UI Logon UI  
 {7998DC37-D3FE-487C-A60A-7701FCC70CC6} Microsoft WBEM A51 Repository  
 {7999FC25-D3C6-11CF-ACAB-00A024A55AEF} COM+ Transaction Context Component  
 {79eac9d0-baf9-11ce-8c82-00aa004ba90b} StdHlink  
 {79eac9d1-baf9-11ce-8c82-00aa004ba90b} StdHlinkBrowseContext  
 {7A0CC021-2939-4379-AA82-12AECC3538F6} CLSID\_INewsGroupHelp  
 {7A0F6AB7-ED84-46B6-B47E-02AA159A152B} Simple Conflict Presenter  
 {7A56C4CB-D678-4188-85A8-BA2EF68FA10D} SAMI Byte Stream Handler  
 {7A7C3277-8F84-4636-95B2-EBB5507FF77E} LatLongReport Class  
 {7A80E4A8-8005-11D2-BCF8-00C04F72C717} ExtractIcon Class  
 {7A9D77BD-5403-11d2-8785-2E0420524153} User Accounts  
 {7aa7790d-75d7-484b-98a1-3913d022091d} Shell FMIFS Wrapper  
 {7abbbcca-e01b-4560-8228-92e1eedbc908} CLSID\_CopyUndoHandler  
 {7AD84985-87B4-4a16-BE58-8B72A5B390F7} PlayTo  
 {7AFA253E-F823-42f6-A5D9-714BDE467412} AVI Byte Stream Handler  
 {7B19A919-A9D6-49E5-BD45-02C34E4E4CD5}  
 {7B2801E6-0BC6-4c92-B742-6BE9B01AE874} DllHostInitializer

## SOFTWARE OUTPUT

{7B31547E-EF7E-479b-9494-2216DC179E61}	Autoplay Handler
{7B3BC2A0-AA50-4ae7-BD44-B03649EC87C2}	VPS Decoder
{7b4a83b6-f704-4b77-8e3d-c6087e3a21d2}	Share Command State Handler
{7B5A12E8-0C60-4939-A046-11CF879B19FB}	WlanDlg Get Key Task Class
{7b81be6a-ce2b-4676-a29e-eb907a5126c5}	Programs and Features
{7b9e38b0-a97c-11d0-8534-00c04fd8d503}	ADs Property Value Object
{7BA4C740-9E81-11CF-99D3-00AA004AE837}	Microsoft SendTo Service
{7bafb3b1-d8f4-4279-9253-27da423108de}	WMV Screen decoder DMO
{7be73787-ce71-4b33-b4c8-00d32b54bea8}	HomeGroup Password
{7be9d83c-a729-4d97-b5a7-1b7313c39e0a}	Programs Folder
{7C07E0D0-4418-11D2-9212-00C04FBBBFB3}	MSPersist
{7C23220E-55BB-11D3-8B16-00C04FB6BD3D}	WM ASF Writer
{7c61d0a6-af7e-483a-b705-d2c5c2264656}	CLSID_EverywhereScopeFiller
{7C857801-7381-11CF-884D-00AA004B2E24}	PSFactoryBuffer
{7CB359C5-570F-43c6-971F-1DB499EE57A1}	WMPPlayer PlaybackPropPage Class
{7cd3c903-d2e9-4a4d-8af3-3025445b24bf}	FilterControl
{7D096C5F-AC08-4F1F-BEB7-5C22C517CE39}	Windows Search Manager
{7d13f939-b90e-42ea-8fb6-c2183f14c578}	Redo command invocation
{7D22E920-5CA9-4787-8C2B-A6779BD11781}	
{7D3195FF-A16A-43c3-9E50-E8A0975B234C}	BTHPAN Device Center Context Menu Handler
{7D8AA343-6E63-4663-BE90-6B80F66540A3}	VMR ImageSync
{7D9239E5-782C-4126-99AD-81F0E8DA8F5C}	New Network category Options Page
{7d9ad905-b754-4297-b2eb-8371abe25540}	Adhoc Networks Exists Page
{7DB7A939-E5C8-4eaa-B3E0-43CE04CAFFBE}	
{7df2cfcd-6c09-415a-ae9d-5263f4964cbb}	CLSID_SortColumnArray
{7DF62B50-6843-11D2-9EEB-006008039E37}	Generate Still Video
{7DF8EF76-D449-485f-B4EB-58DC96B31EDB}	HomeGroup Printing Device Class
{7e320092-596a-41b2-bbeb-175d10504eb6}	WMVideo8 Encoder DMO
{7E37D5E7-263D-45CF-842B-96A95C63E46C}	Group Policy Object Proxy Stub
{7E3FCEA1-31B4-11D2-AE1F-0080C7337EA1}	XML Viewer Moniker
{7E4A23E2-B969-4761-BE35-1A8CED58E323}	XPS Thumbnail Generator
{7E66DBEF-2474-4E82-919B-9A855F4C2FE8}	WscIsvIf Proxy Stub
{7e99c0a3-f935-11d2-ba96-00c04fb6d0d1}	ADs DN With Binary Object
{7E9D8D44-6926-426F-AA2B-217A819A5CCE}	XML File Persistent Handler
{7EB5FBE4-2100-49E6-8593-17E130122F91}	Fade Task
{7F1899DA-62A6-11D0-A2C6-00C04FD909DD}	ScopeTree 1.0 Object
{7F368827-9516-11D0-83D9-00A0C911E5DF}	Microsoft Server Configuration Notify
Object	
{7F43B400-1A0E-4D57-BBC9-6B0C65F7A889}	PSFactoryBuffer
{7F598975-37E0-4A67-A992-116680F0CEDA}	Microsoft WMI Provider Subsystem Self
Instrumentation	
{7f5d25f8-78a5-49a8-a33c-2c0e11831c66}	WMDRM Context
{7F72CC7A-74A0-45B4-909C-14FB8186DD7E}	WBEM IP DFS Provider
{7F73B8F6-C19C-11D0-AA66-00C04FC2EDDC}	
{7f8e7858-c362-4c0a-b868-4cdd929da715}	Authentication UI User Settings
{7F9CB14D-48E4-43B6-9346-1AEBC39C64D3}	MS Video Control Closed Captioning Feature
Segment	
{7FE0D935-DDA6-443F-85D0-1CFB58FE41DD}	PSFactoryBuffer

## SOFTWARE OUTPUT

```

{7febaf7c-18cf-11d2-993f-00a0c91f3880} DefView Persistent history
{80009818-f38f-4af1-87b5-eadaab9433e58} MF ADTS Property Handler
{804c8e4a-3dae-460d-90ad-8694b510f851} Microsoft IME IMEPad Server
{807553E6-5146-11D5-A672-00B0D022E945}
{8078DA75-F43F-341D-A00E-20D6D736415E}
{8082C5E6-4C27-48ec-A809-B8E1122E8F97} .contact shell extension handler
{8086ebd4-43e3-4b19-beb3-f0ea4ecf319c} CScriptedDiagNativeHost
{809B6661-94C4-49E6-B6EC-3F0F862215AA} Collection of BDA Tuning Model

Components(Broadcast Substreams)
{80c68d96-366b-11dc-9eaa-00161718cf63} Play command invocation
{80F3F1D5-FECA-45F3-BC32-752C152E456E} Tablet PC Settings Control Panel
{80F94176-FCCC-11D2-B991-00C04F8ECD78} MessageView Class
{81007291-f070-4c4f-b978-ad1bec84babcb} Rename command invocation
{8144B6F5-20A8-444a-B8EE-19DF0BB84BDB} StiEventHandler Class
{814B9800-1C88-11D1-BAD9-00609744111A} VBI Surface Allocator
{814B9801-1C88-11D1-BAD9-00609744111A} VideoPort VBI Object
{81796171-DF5F-4F1B-A80C-BE4715D3C6BB} TextNormMultiResult Class
{819469D2-D0CF-11d1-8E0B-00C04FC2E0C7}
{819d1334-9d74-4254-9ac8-dc745ebc5386} InfoBar Manager
{81b43e73-e814-4dcd-a7c6-e22e7fe6a029} Item Store Object
{81BD8EE8-F713-36A5-B7D5-9E92ACB4A18A}
{81E9DD62-78D5-11D2-B47E-006097B3391B} DVcrControl Property Page
{820825FD-1358-4705-8FEB-56B5CEE8BFD5} NULL SSID INFO PAGE
{823535A0-0318-11D3-9D8E-00C04F72D980} BDA Tuning Model Component Type Class

(Broadcast Substream Type)
{823B8267-735C-477E-8151-0FA9ADC8AB3A} Convert ACL to SIDs and resolve SIDs
{82435bdf-f7c1-4df9-8103-eeabebf3d6e1} WMDRM Content Enabler
{8278F931-2A3E-11d2-838F-00C04FD918D0} Tracking Shell Menu
{82BD0E67-9FEA-4748-8672-D5EFE5B779B0}
{82c588e7-e54b-408c-9f8c-6af9adf6f1e9} FormatForDisplay Helper
{82d353df-90bd-4382-8bc2-3f6192b76e34} WMVideo Decoder DMO
{82d792e9-8f8c-4f4a-9dbf-06253e4562a8} FilterWorkerItem
{8336e323-2e6a-4a04-937c-548f681839b3} X509 Certificate Template AD Writable
{8352E327-B2EC-3331-9998-817EC5CC93B8}
{836FA1B6-1190-4005-B434-7ED921BE2026} UserDictionary Class
{8398EE59-134A-420A-934A-D86A7F900D9A} IsdbString Class
{83bb272f-7d5e-4b6e-9250-889893f0dac7} Folder options command
{83bbcbf3-b28a-4919-a5aa-73027445d672}
{83BC5EC0-6F2A-11d0-A1C4-00AA00C16E65}
{842D84C9-C347-11D1-8F64-00C04FB611C7} Interface Proxy Stub
{84a3a6bf-f1d8-496e-9f05-d3de70973152} WWan Helper Class
{84D586C4-A423-11D2-B943-00C04F79D22F} CustRg Class
{84e04a55-2d42-4909-86e3-62fd11483e8b} Temporary Setup Files Cleanup
{84FC747A-1940-3D85-8819-EA53FC73DB1B}
{85074451-173D-4091-8648-C0E196BB363E} WSUS App Publisher
{8509bb76-ffa3-4827-ba5e-2e786010f42f} Item Set Operations Object
{850D1D11-70F3-4BE5-9A11-77AA6B2BB201} CommonDialog Class
{85131630-480C-11D2-B1F9-00C04F86C324} JS File Host Encode Object

```



## SOFTWARE OUTPUT

{85131631-480C-11D2-B1F9-00C04F86C324} VBS File Host Encode Object  
 {854CB94F-2279-4F7F-AC62-31E22E4D8899} InfraConnectTask  
 {8570b44e-d109-42d3-be32-0f8d446669c5} Close window command invocation  
 {85862EDA-F507-4d5b-ACA9-BB2C34A85682} Microsoft XPS Rich Preview Handler  
 {8596E5F0-0DA5-11D0-BD21-00A0C911CE86} File Writer  
 {85BBD920-42A0-1069-A2E4-08002B30309D} Briefcase  
 {85cfccaf-2d14-42b6-80b6-f40f65d016e7} Shortcut  
 {85e94d25-0712-47ed-8cde-b0971177c6a1} Microsoft DocProp Rating Control  
 {85EB7D1F-7431-3E1E-A26E-EB1D16CB4ABB} MS IME 10 Character Applet  
 {860D36EE-748E-4B73-AE45-C33187E6F166} Closed Captions Analysis Feature Segment  
 {86151827-E47B-45ee-8421-D10E6E690979} Remote Printers  
 {863aa9fd-42df-457b-8e4d-0de1b8015c60} SvcVwr 1.0 Object  
 {863FA3AC-9D97-4560-9587-7FA58727608B} Network Context Menu Extension  
 {86422020-42A0-1069-A2E5-08002B30309D} User Event Timer  
 {864A1288-354C-4D19-9D68-C2742BB14997} Programs Folder and Fast Items  
 {865e5e76-ad83-4dca-a109-50dc2113ce9a} PSFactoryBuffer  
 {8664DA16-DDA2-42AC-926A-C18F9127C302} DirectShow Plugin Manager  
 {8670C736-F614-427b-8ADA-BBADC587194B} Briefcase Folder  
 {86747AC0-42A0-1069-A2E6-08002B30309D} WlanConn LUA  
 {868A2E25-D6C1-450b-8510-734A4AFEE8BC} Application Document Lists  
 {86bec222-30f2-47e0-9f25-60d11cd75c28} Application Destination List  
 {86c14003-4d6b-4ef3-a7b4-0506663b2e68} .exe drop target  
 {86C86720-42A0-1069-A2E8-08002B30309D} Virtual Factory for Usercpl  
 {86d5eb8a-859f-4c7b-a76b-2bd819b7a850} CElevateWlanUi  
 {86F80216-5DD6-4F43-953B-35EF40A35AEE} FaxTiff Class  
 {87099231-C7AF-11D0-B225-00C04FB6C2F5} Audio Media Properties Handler  
 {875CB1A1-0F29-45de-A1AE-CFB4950D0B78} Mobile Broadband Profile Settings Editor  
 {87630419-6216-4ff8-a1f0-143562d16d5c} InkRecognizerGuide Class  
 {8770D941-A63A-4671-A375-2855A18EBA73} File Backup Index  
 {877A0BB7-A313-4491-87B5-2E6D0594F520} Plug In Distributor: IKsClock  
 {877ca5ac-cb41-4842-9c69-9136e42d47e2} HomeGroup Task  
 {877E4351-6FEA-11D0-B863-00AA00A216A1} ThirdPartyEapDispatcherPeerRuntime  
 {879fb53b-cba3-4fc8-b233-d9a93afa7fbc} Indexing Options Control Panel  
 {87BB326B-E4A0-4de1-94F0-B9F41D0C6059} DirectSoundWavesReverbDMO  
 {87DB1ADA-AA39-11D1-829F-00A0C906B239} State of play command  
 {87FC0268-9A55-4360-95AA-004A1D9DE26C} Location Association List  
 {880ac964-2e34-4425-8cf2-86ada2c3a019} Summary Properties Page  
 {8821c0e8-73ba-4448-8b46-23824e0d7831} SrControl Class  
 {883373C3-BF89-11D1-BE35-080036B11A03} LogonPasswordReset  
 {883FF1FC-09E1-48e5-8E54-E2469ACB0CFD} ObjectId  
 {8841d728-1a76-4682-bb6f-a9ea53b4b3ba} ObjectId Collection  
 {884e2000-217d-11da-b2a4-000e7bbb2b09} Binary Converter  
 {884e2001-217d-11da-b2a4-000e7bbb2b09} X500 Distinguished Name  
 {884e2002-217d-11da-b2a4-000e7bbb2b09} Csp Information  
 {884e2003-217d-11da-b2a4-000e7bbb2b09} Csp Information Collection  
 {884e2007-217d-11da-b2a4-000e7bbb2b09}  
 {884e2008-217d-11da-b2a4-000e7bbb2b09}

## SOFTWARE OUTPUT

{884e2009-217d-11da-b2a4-000e7bbb2b09}	Csp Status
{884e200b-217d-11da-b2a4-000e7bbb2b09}	X509 Public Key
{884e200c-217d-11da-b2a4-000e7bbb2b09}	X509 Private Key
{884e200d-217d-11da-b2a4-000e7bbb2b09}	X509 Extension
{884e200e-217d-11da-b2a4-000e7bbb2b09}	X509 Extension Collection
{884e200f-217d-11da-b2a4-000e7bbb2b09}	X509 Extension Key Usage
{884e2010-217d-11da-b2a4-000e7bbb2b09}	X509 Extension Enhanced Key Usage
{884e2011-217d-11da-b2a4-000e7bbb2b09}	X509 Extension Template Name
{884e2012-217d-11da-b2a4-000e7bbb2b09}	X509 Extension Template
{884e2013-217d-11da-b2a4-000e7bbb2b09}	Alternative Name
{884e2014-217d-11da-b2a4-000e7bbb2b09}	Alternative Name Collection
{884e2015-217d-11da-b2a4-000e7bbb2b09}	X509 Extension Alternative Names
{884e2016-217d-11da-b2a4-000e7bbb2b09}	X509 Extension Basic Constraints
{884e2017-217d-11da-b2a4-000e7bbb2b09}	X509 Extension Subject Key Identifier
{884e2018-217d-11da-b2a4-000e7bbb2b09}	X509 Extension Authority Key Identifier
{884e2019-217d-11da-b2a4-000e7bbb2b09}	Smime Capability
{884e201a-217d-11da-b2a4-000e7bbb2b09}	Smime Capabilities Collection
{884e201b-217d-11da-b2a4-000e7bbb2b09}	X509 Extension Smime Capabilities
{884e201c-217d-11da-b2a4-000e7bbb2b09}	Policy Qualifier
{884e201d-217d-11da-b2a4-000e7bbb2b09}	Policy Qualifier Collection
{884e201e-217d-11da-b2a4-000e7bbb2b09}	Certificate Policy
{884e201f-217d-11da-b2a4-000e7bbb2b09}	Certificate Policies Collection
{884e2020-217d-11da-b2a4-000e7bbb2b09}	X509 Extension Certificate Policies
{884e2021-217d-11da-b2a4-000e7bbb2b09}	X509 Extension MS Application Policies
{884e2022-217d-11da-b2a4-000e7bbb2b09}	X509 Attribute
{884e2023-217d-11da-b2a4-000e7bbb2b09}	X509 Attribute Collection
{884e2024-217d-11da-b2a4-000e7bbb2b09}	X509 Attribute Extensions
{884e2025-217d-11da-b2a4-000e7bbb2b09}	X509 Attribute ClientId
{884e2026-217d-11da-b2a4-000e7bbb2b09}	X509 Attribute Renewal Certificate
{884e2027-217d-11da-b2a4-000e7bbb2b09}	X509 Attribute Archivekey
{884e2028-217d-11da-b2a4-000e7bbb2b09}	X509 Attribute Archivekeyhash
{884e202a-217d-11da-b2a4-000e7bbb2b09}	X509 Attribute OS Version
{884e202b-217d-11da-b2a4-000e7bbb2b09}	X509 Attribute Csp Provider
{884e202c-217d-11da-b2a4-000e7bbb2b09}	Cryptographic Attribute
{884e202d-217d-11da-b2a4-000e7bbb2b09}	Cryptographic Attribute Collection
{884e202e-217d-11da-b2a4-000e7bbb2b09}	Certificate Property
{884e202f-217d-11da-b2a4-000e7bbb2b09}	Certificate Properties Collection
{884e2030-217d-11da-b2a4-000e7bbb2b09}	Certificate Property Friendly Name
{884e2031-217d-11da-b2a4-000e7bbb2b09}	Certificate Property Description
{884e2032-217d-11da-b2a4-000e7bbb2b09}	Certificate Property Auto-Enroll
{884e2033-217d-11da-b2a4-000e7bbb2b09}	Certificate Property Request Originator
{884e2034-217d-11da-b2a4-000e7bbb2b09}	Certificate Property SHA-1 Hash
{884e2036-217d-11da-b2a4-000e7bbb2b09}	Certificate Property Key Provider
Information	
{884e2037-217d-11da-b2a4-000e7bbb2b09}	Certificate Property Archived
{884e2038-217d-11da-b2a4-000e7bbb2b09}	Certificate Property Backed-Up
{884e2039-217d-11da-b2a4-000e7bbb2b09}	Certificate Property Enrollment
{884e203a-217d-11da-b2a4-000e7bbb2b09}	Certificate Property Renewal

## SOFTWARE OUTPUT

{884e203b-217d-11da-b2a4-000e7bbb2b09}	Certificate Property Archived Key Hash
{884e203d-217d-11da-b2a4-000e7bbb2b09}	Signer Certificate
{884e203f-217d-11da-b2a4-000e7bbb2b09}	Name Value Pair
{884e2042-217d-11da-b2a4-000e7bbb2b09}	X509 CertificateRequest Pkcs10
{884e2043-217d-11da-b2a4-000e7bbb2b09}	X509 CertificateRequest Certificate
{884e2044-217d-11da-b2a4-000e7bbb2b09}	X509 CertificateRequest PKcs7
{884e2045-217d-11da-b2a4-000e7bbb2b09}	X509 CertificateRequest Cmc
{884e2046-217d-11da-b2a4-000e7bbb2b09}	X509 Enrollment
{884e2049-217d-11da-b2a4-000e7bbb2b09}	X509 Enrollment WebClassFactory
{884e204c-217d-11da-b2a4-000e7bbb2b09}	Certificate Property Enrollment Policy

Server

{884e2050-217d-11da-b2a4-000e7bbb2b09}	X509 Enrollment Helper
{884e2051-217d-11da-b2a4-000e7bbb2b09}	X509 Machine Enrollment Factory
{8854F6A0-4683-4AE7-9191-752FE64612C3}	InkDivider Class
{8872FF1B-98FA-4D7A-8D93-C9F1055F85BB}	ATSC Tune Request Location Information
{88d96a05-f192-11d4-a65f-0040963251e5}	XML DOM Document 6.0
{88d96a06-f192-11d4-a65f-0040963251e5}	Free Threaded XML DOM Document 6.0
{88d96a07-f192-11d4-a65f-0040963251e5}	XML Schema Cache 6.0
{88d96a08-f192-11d4-a65f-0040963251e5}	XSL Template 6.0
{88d96a0a-f192-11d4-a65f-0040963251e5}	XML HTTP 6.0
{88d96a0b-f192-11d4-a65f-0040963251e5}	Server XML HTTP 6.0
{88d96a0c-f192-11d4-a65f-0040963251e5}	SAX XML Reader 6.0
{88d96a0e-f192-11d4-a65f-0040963251e5}	SAXAttributes 6.0
{88d96a0f-f192-11d4-a65f-0040963251e5}	MXXMLWriter 6.0
{88d96a10-f192-11d4-a65f-0040963251e5}	MXHTMLWriter 6.0
{88d96a11-f192-11d4-a65f-0040963251e5}	MXNamespaceManager 6.0
{896664F7-12E1-490f-8782-C0835AFD98FC}	Libraries delegate folder that appears in

Users Files Folder

{89BCB7A4-6119-101A-BCB7-00DD010655AF}	
{89BCB7A5-6119-101A-BCB7-00DD010655AF}	
{89BCB7A6-6119-101A-BCB7-00DD010655AF}	
{89C2E132-C29B-11DB-96FA-005056C00008}	PBDA PTFilter
{89D83576-6BD1-4c86-9454-BEB04E94C819}	@%systemroot%\system32\mssvp.dll,-110
{89F9F7B0-8DE3-4AE0-8B41-109ABAB32151}	Microsoft WBEM Message Multi SendReceive
{8A01C400-A3E0-4F8D-A933-FF780F22BD87}	SnapinComponentData Class
{8A03E749-672E-446E-BF1F-2C11D233B6FF}	
{8A22069C-1EF7-45D2-A409-219540D00A76}	Infrastructure Connect Page Class
{8A23E65E-31C2-11d0-891C-00A024AB2DBB}	
{8A3E2E1E-A40B-4650-9FB4-30072A68E661}	ParseTracer Class
{8A667154-F9CB-11D2-AD8A-0060B0575ABC}	Microsoft DirectSound Wave
{8A674B49-1F63-11D3-B64C-00C04F79498E}	Utility Object for creating a Property Bag

backed by the Registry

{8A674B4C-1F63-11D3-B64C-00C04F79498E}	BDA Tuning Model Analog Radio Tuning Space
{8A674B4D-1F63-11D3-B64C-00C04F79498E}	BDA Tuning Model Analog TV Tuning Space
{8A6842BB-84DB-4EFA-99B9-06C850DF53FC}	WMPlayer NetworkPropPage Class
{8A734961-C4AA-4741-AC1E-791ACEBF5B39}	
{8ac3587a-4ae7-42d8-99e0-0a6013eef90f}	Device Proxy MFT
{8ADD018C-5C5F-43C5-BE1E-07BAE85593B7}	HomeGroup Alpha Hosted Listener

## SOFTWARE OUTPUT

{8ADE5386-8E9B-4F4C-ACF2-F0008706B238}  
 {8B7FBFE0-5CD7-494a-AF8C-283A65707506} Default Location Class  
 {8BC3F05E-D86B-11D0-A075-00C04FB68820} Windows Management and Instrumentation  
 {8be9f5ea-e746-4e47-ad57-3fb191ca1eed} Listview Popup  
 {8BEBCE8B-1AF0-4323-8B4D-36994567CAE1} Microsoft WMI Provider Subsystem InProc  
 Factory  
 {8bf9a910-a8ff-457f-999f-a5ca10b4a885} Smartcard Credential Provider  
 {8c1645b0-9864-465e-be75-990b030e4b11} XWizard Factory Generated Class (HomeGroup  
 Join Hook Page)  
 {8C334A55-DDB9-491c-817E-35A6B85D2ECB}  
 {8C482DCE-2644-4419-AEFF-189219F916B9} HostPeerApis  
 {8c4fb173-81ae-4399-9208-591a574a893f} Mobile Broadband CFE Page Class  
 {8c4fce56-fc9a-4fcb-bd35-2ccabfd93844} Authentication UI Logon Settings  
 {8C7461EF-2B13-11d2-BE35-3078302C2030} DEPRECATED: Component Categories cache  
 daemon  
 {8c7eaf13-fbd6-4ed8-ac79-fb12fcd71326} SdEngine2 Class  
 {8C89071F-452E-4E95-9682-9D1024627172}  
 {8C9E8E1C-90F0-11D1-BA0F-00A0C906B239}  
 {8CBEED49-18A6-4D9C-8EF5-E4DD9AB04A83} Windows Media Player  
 WMEncSourcePluginCommunicator Class  
 {8CF89BCB-394C-49b2-AE28-A59DD4ED7F68} PSFactoryBuffer  
 {8D04238E-9FD1-41C6-8DE3-9E1EE309E935} MSVidCtl DVD to Audio Renderer Composition  
 Segment  
 {8D1C559D-84F0-4BB3-A7D5-56A7435A9BA6} Microsoft WBEM WMI Object Factory  
 {8d1e5d4b-a99c-4408-b0f0-ccab9e5835a1} SuggestFilterWorker  
 {8D26D9AA-5DA8-4b95-949A-B74954A229A6} Virtual Factory for Action Center CPL  
 {8D4B04E1-1331-11d0-81B8-00C04FD85AB4} CLSID\_ImmAccountManager  
 {8d80504a-0826-40c5-97e1-ebc68f953792} OLE DocFile Property Handler  
 {8D8B8E30-C451-421B-8553-D2976AFA648C} Sync Center Schedule Wizard  
 {8DA6DB1C-8114-40c6-9D97-D2E7E9757D67} PSFactoryBuffer  
 {8DB2180F-BD29-11D1-8B7E-00C04FD7A924} COMComponentRegistrar Class  
 {8DE9C74C-605A-4acd-BEE3-2B222AA2D23D} NegationCondition Class  
 {8e35b548-f174-4c7d-81e2-8ed33126f6fd} Biometrics navigate target object  
 {8E528C21-9D52-4030-BA92-3481227ADDD1} WMPPlayer PrivacyPropPage Class  
 {8e827c11-33e7-4bc1-b242-8cd9a1c2b304} Merged Folder Categorizer  
 {8e85d0ce-deaf-4ea1-9410-fd1a2105ceb5} Microsoft DocProp Inplace Multi-Value  
 Property Control  
 {8e87e7b8-896b-4e67-bfa2-45c67d60ac3a} CPL Search Target Services  
 {8E8F1601-AE98-3DAC-B48B-EC27C95A481E}  
 {8E974B5A-A286-37DA-94F8-5872C500EB0E}  
 {8EE97210-FD1F-4b19-91DA-67914005F020} Microsoft DocProp Inplace ML Edit Box  
 Control  
 {8F0C5675-AEEF-11d0-84F0-00C04FD43F8F} AthWafer  
 {8F914656-9D0A-4EB2-9019-0BF96D8A9EE6}  
 {8FADC6A8-183E-4DFC-944A-84A323334B98} CFindNetPrinters Class  
 {90087284-d6d6-11d0-8353-00a0c90640bf} Device Manager extension  
 {900be39d-6be8-461a-bc4d-b0fa71f5ecb1} DiagnosticInfrastructureCustomHandler  
 {900c0763-5cad-4a34-bc1f-40cd513679d5} User Account Control Check Service

## SOFTWARE OUTPUT

{905667aa-acd6-11d2-8080-00805f6596d2}  
 {905b55a8-77f0-4d28-80dd-e46b1412343f} Execute OpenSearch view site command  
 {90AA3A4E-1CBA-4233-B8BB-535773D48449} Taskband Pin  
 {90b9bce2-b6db-4fd3-8451-35917ea1081b} CLSID\_SearchMSExecute  
 {90BE9587-37b7-477C-81A7-BA7C5C40FF81} MSASR Locale Handler Class (2057)  
 {90F18417-F0F1-484E-9D3C-59DCEEE5DBD8} CIEAxiInstallerService Class  
 {90f8c90b-04e0-4e92-a186-e6e9c125d664} Property Labels  
 {913a6daa-57ee-4551-9ada-64d329d306a5} App Locations Icon Extract Extension  
 {914feed8-267a-4baa-b8aa-21e233792679} Microsoft Preview Creator  
 {91778246-9BE4-4713-A651-E833B853CC30}  
 {91888BF6-FED1-4acd-9CB1-6C2F80AE58A3}  
 {9193A8F9-0CBA-400E-AA97-EB4709164576} MSVidCtl SBE Source to Closed Caption  
 Composition Segment  
 {91f39027-217f-11da-b2a4-000e7bbb2b09} X509 Enrollment Policy Active Directory  
 {91f39028-217f-11da-b2a4-000e7bbb2b09} X509 Enrollment Policy Web Service  
 {91f39029-217f-11da-b2a4-000e7bbb2b09} X.509 Policy Server List Manager Class  
 {91f3902a-217f-11da-b2a4-000e7bbb2b09} X.509 Policy Server URL Class  
 {9200689A-F979-4eea-8830-0E1D6B74821F} Virtual Factory for Recovery  
 {92038079-b9ef-428f-87f0-0463fcb1272a} CLSID\_VisibleIn  
 {9207d8c7-e7c8-412e-87f8-2e61171bd291} Autoplay Known Devices Info  
 {92187326-72B4-11d0-A1AC-0000F8026977} Game Controllers CPL Shell Extension  
 Default Property Sheets  
 {92337A8C-E11D-11D0-BE48-00C04FC30DF6} prturl Class  
 {92396AD0-68F5-11d0-A57E-00A0C9138C66} RowsetHelper  
 {923BFC9D-0F16-4B02-AF1B-39A2504D9873} Additional Information Page Class  
 {92498132-4D1A-4297-9B78-9E2E4BA99C07} NSSManager Class  
 {924ccc1b-6562-4c85-8657-d177925222b6} Desktop Gadget Helper API  
 {9264B7DC-A82F-4AFD-89C8-4F399DA7B028} VAN Settings Page Class  
 {926f41f7-003e-4382-9e84-9e953be10562} ADTS Byte Stream Handler  
 {9271B890-7BBF-48DB-ACB3-F973DC34156D} PSFactoryBuffer  
 {927971f5-0939-11d1-8be1-00c04fd8d503} ADs Large Integer Object  
 {92A5010F-4404-4035-8D53-B87F5A736809}  
 {92ab5af7-a374-417e-b2e2-9b317353a322} Microsoft Library Boolean Check Mark  
 Control  
 {92ad68ab-17e0-11d1-b230-00c04fb9473f} STClient Class  
 {92b66080-5e2d-449e-90c4-c41f268e5514} G711 ACM Wrapper MFT  
 {92B94828-1AF7-4e6e-9EBF-770657F77AF5} Custom Composition Segment from iTV to  
 Stream Buffer Source  
 {92c85649-0892-4bc7-9b63-949f64149a26} CMigrationPlugin Object  
 {92CC85F4-ACA4-4D72-94C8-49D1CAD0985F} Infrastructure Connected Page Class  
 {92D2CC58-4386-45a3-B98C-7E0CE64A4117} PSFactoryBuffer  
 {92dbad9f-5025-49b0-9078-2d78f935e341} CLSID\_PreviewMime  
 {92ED88BF-879E-448f-B6B6-A385BCEB846D} MS Video Control Closed Captioning SI  
 Feature Segment  
 {9301E380-1F22-11D3-8226-D2FA76255D47} DirectMusicContainer  
 {93126582-5402-4DB1-A102-33D330BC9B69} Windows Media Player  
 WMEnc5Point1WavSourcePropertyPage Class  
 {9324DA94-50EC-4A14-A770-E90CA03E7C8F} Windows Theme Manager 2 API

## SOFTWARE OUTPUT

```

{9343812e-1c37-4a49-a12e-4b2d810d956b} CLSID_SearchHome
{934a7048-1e4a-4d6e-9a9a-cb739f519b07} XWizard Factory Generated Class (HomeGroup
Change Sharing Hook Page)
{934D4698-6A59-48f8-9F29-9FB30670320E} Structured Query Helper Class
{93714ED0-53F0-11D2-9EE6-006008039E37} Frame Rate Converter
{937C1A34-151D-4610-9CA6-A8CC9BDB5D83} InkObject Class
{9381AF33-66A3-4D5A-8AF2-9515B1DC19A5} PSFactoryBuffer
{93A094D7-51E8-485b-904A-8D6B97DC6B39} SBE2 File Reader
{93a56381-e0cd-485a-b60e-67819e12f81b} CLSID_CommonExplorerHost
{93AF0C51-2275-45D2-A35B-F2BA21CAED00}
{94297043-BD82-4DFD-B0DE-8177739C6D20} DMO Wrapper Filter
{942B7909-A28E-49a1-A207-34EBCBCB4B3B} MSVidCtl Analog Capture to CCA Composition
Segment
{942bc614-676c-464e-b384-d3202aaa02da} INI Property Set Storage Handler
{94357B53-CA29-4b78-83AE-E8FE7409134F} Drive Size Categorizer
{94426DE2-3211-11d2-A0DB-00C04F8EDCEE}
{944D4C00-DD52-11CE-BF0E-00AA0055595A} DirectDraw Property Page
{9456A480-E88B-43EA-9E73-0B2D9B71B1CA}
{94596c7e-3744-41ce-893e-bbf09122f76a} Smartcard Pin Provider
{948B45F7-EFB8-46fb-8704-B340D847227A} Location Description Property Handler
{94AB5C27-C954-4218-B0A1-29640412EFBE}
{94abaf2a-892a-11d1-bbc4-00a0c90640bf} About Device Manager
{94E03510-31B9-47a0-A44E-E932AC86BB17} Windows Media Player Device Autoplay
{956FADED-2450-4ABB-9F8C-4629FAFEBB92} HomeGroup Encryption
{95876EB0-90F0-11D1-BA0F-00A0C906B239}
{958A1709-3B44-11D1-AD74-00C04FC2ADC0} RM Enlistment Helper
{958C59A0-3670-4FE0-B893-6998BB494402} Microsoft WBEM Smart Object Marshaler
{95A18FCB-6850-420F-979B-CB3A149F2CC8} EnumSTSALTINFO Class
{95CE8412-7027-11D1-B879-006008059382} Shell Tree Walker
{961C1130-89AD-11CF-88A1-00AA004B9986}
{96236A71-9DBC-11DA-9E3F-0011114AE311} PSFactoryBuffer
{96236A85-9DBC-11DA-9E3F-0011114AE311} RdcLibrary Class
{96236A8F-9DBC-11DA-9E3F-0011114AE311} SimilarityTraitsTable Class
{96236A90-9DBC-11DA-9E3F-0011114AE311} SimilarityFileIdTable Class
{96236A91-9DBC-11DA-9E3F-0011114AE311} Similarity Class
{967696C6-354C-4B5C-9CC8-BD9E1C480C77} PimcSurrogate Class
{9694E38A-E081-46ac-99A0-8743C909ACB6} html persistent handler for mapi email
{96AE8D84-A250-4520-95A5-A47A7E3C548B} Parental Controls
{96BEC059-2052-4e44-8E11-123ACDC936FE} WMDM Sync Property Page
{96FAC3B9-0273-4c0d-84F0-3A207A5EB38B} Network Map
{97103AE5-6248-4E04-97B5-36663159967C} Windows Media Player WMEncTunerPropPage
Class
{973A7390-2608-3943-9015-D798D1217C08}
{9743B50B-3190-4061-8DA3-BE13AA02181E} Infrastructure Progress Page Class
{975ABEDC-F64B-436d-ABFF-44B932459856} Windows Media Player OCXAdvancedPropPage
Class
{97e467b4-98c6-4f19-9588-161b7773d6f6} Office Document Property Handler
{97EFC6C3-695B-4637-A6E6-9A28895F410E} PSFactoryBuffer

```

## SOFTWARE OUTPUT

```

{98037168-078f-4e5a-b235-a41aa5fd3bf5} WMPMDE MPEG2 SINK ACTIVATE
{98042251-8C2B-4FC4-93E2-B1DB331EF5B9} WMPlayer AdvancedPropPage Class
{98230571-0087-4204-b020-3282538e57d3} Color Converter DMO
{98455561-5136-4d28-AB08-4CEE40EA2781} MF Video Presenter
{987BBF42-5500-46D6-BAF0-A825828BC4EF} Windows Media Player WMEncFileSource Class
{989D1DC0-B162-11D1-B6EC-D27DDCF9A923} XML Script Engine
{98af66e4-aa41-4226-b80f-0b1a8f34eeb4} Manifest mime handler
{98AFF3F0-5524-11D0-8812-00A0C903B83C} CertRequest Class
{98de59a0-d175-11cd-a7bd-00006b827d94} Microsoft Office Persistent Handler
{98F63271-6C09-48B3-A571-990155932D0B} FaxControl Class
{991DA7E5-953F-435B-BE5E-B92A05EDFC42} MSVidCtl Stream Buffer Source To Generic

Sink Composition segment
{992CFFA0-F557-101A-88EC-00DD010CCC48} Network Connections
{995C996E-D918-4a8c-A302-45719A6F4EA7} Shell Hardware Mixed Content Handler
{996d2d72-4c19-47f8-8f58-0bb13e80a659} HomeGroup Balloon
{99969a8f-27e6-4adf-ab9f-b5b5e90d4733} Verb Handler for launching verbs on
properties of items
{99c0179c-c20c-488c-a510-bd779b9376ae}
{99cdfdaf-3573-4d97-bc06-d7c36627edef} Mobile Broadband Connect Failure Page
Class
{99D54F63-1A69-41AE-AA4D-C976EB3F0713} VMR Allocator Presenter
{99E89F48-A745-416d-A4E0-ECF53C65DFA0} DynamicRenderer Class
{99EB9580-04EC-4B4C-99F5-52B616D444D9} MSASR Locale Handler Class (1031)
{9a02e012-6303-4e1e-b9a1-630f802592c5} Packed Property Storage Object
{9A5EA990-3034-4D6F-9128-01F3C61022BC} GameExplorer Class
{9A653086-174F-11D2-B5F9-00104B703EFD} Microsoft WBEM WBEM Class Object
{9a97f12a-6b73-4dc4-b3c1-e9244c03adac} shell foreground window setter
{9AA0422B-E5C5-4A6B-ACEC-C96E2E05B353} CIsdb Class
{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917} ShellItem Shell Namespace helper
{9B1F122C-2982-4e91-AA8B-E071D54F2A4D} CAutoUpdate Class 1.0
{9B496CE1-811B-11CF-8C77-00AA006B6814} IAMTimecodeReader
{9B55AA0E-1BC2-46e4-B306-DF9BDFDCC644}
{9B77C0F2-8735-46c5-B90F-5F0B303EF6AB} CAsfTocParser
{9BA05971-F6A8-11CF-A442-00A0C90A8F39} Microsoft Shell Folder View Router
{9BA05972-F6A8-11CF-A442-00A0C90A8F39} ShellWindows
{9BCE6E2B-116B-420F-928B-5356D1629979}
{9BF8D948-5C56-450e-BAF8-D6144C6E81CB} SqlGenerator Class
{9C1CC6E4-D7EB-4EEb-9091-15A7C8791ED9} InkRenderer Class
{9C24A977-0951-451A-8006-0E49BD28CD5F}
{9C502F01-0D36-4f16-8AC9-8693E0D84E44} WMPlayer CDBurnPropPage Class
{9C73F5E5-7AE7-4E32-A8E8-8D23B85255BF} Sync Center Folder
{9CB535DD-4354-42a1-8281-BBB58DEFA741} Performance Control Panel
{9CD31617-B303-4F96-8330-2EB173EA4DC6}
{9CD64701-BDF3-4D14-8E03-F12983D86664} BDA Tuning Model DVB Terrestrial Locator
{9cfc2df3-6ba3-46ef-a836-e519e81f0ec4} Property System Apartment Class Factory
{9D3C0751-A13F-46a6-B833-B46A43C30FE8} MAPI Shell Context Menu
{9D71A98F-1E45-42EC-AF3D-FA13BEFB955C} Manual Connect Page Class
{9D745ED8-C514-4D1D-BF42-751FED2D5AC7} HNetCfg.FwProduct

```

## SOFTWARE OUTPUT

{9DAC2C1E-7C5C-40eb-833B-323E85A1CE84}  
 {9DBD2C50-62AD-11d0-B806-00C04FD706EC} Property Thumbnail Handler  
 {9DCC3CC8-8609-4863-BAD4-03601F4C65E8} LatLongReportFactory Class  
 {9DD35758-AAF5-4894-ADAA-77A492F54E0A} WlanDlgNonUIPage Class  
 {9DE85094-F71F-44f1-8471-15A2FA76FCF3} InkWordList Class  
 {9DFFD99C-536B-4D0F-B70F-E875B78A3477}  
 {9E175B68-F52A-11D8-B9A5-505054503030} Search Gathering Manager  
 {9E175B69-F52A-11D8-B9A5-505054503030} Search Embedded Gathering Manager  
 {9E175B6C-F52A-11D8-B9A5-505054503030} Search Gatherer Transaction  
 {9E175B6D-F52A-11D8-B9A5-505054503030} Search Gatherer Notification  
 {9E175B6E-F52A-11D8-B9A5-505054503030} Microsoft Embedded Search Gatherer  
 Notification  
 {9E175B70-F52A-11D8-B9A5-505054503030} Search Gatherer Language Resource Pool  
 {9E175B74-F52A-11D8-B9A5-505054503030} Search Gatherer Plug-in  
 {9E175B76-F52A-11D8-B9A5-505054503030} Windows Search Service File Protocol  
 Handler  
 {9E175B7F-F52A-11D8-B9A5-505054503030} Search Back off Controller  
 {9E175B8A-F52A-11D8-B9A5-505054503030} Search command creator object  
 {9E175B8B-F52A-11D8-B9A5-505054503030} Windows Search Data Source  
 {9E175B8D-F52A-11D8-B9A5-505054503030} Search FilterRegistration Class  
 {9E175B8E-F52A-11D8-B9A5-505054503030} Search LoadLangRes Class  
 {9E175B90-F52A-11D8-B9A5-505054503030} Full Text SQL Parser  
 {9E175B98-F52A-11D8-B9A5-505054503030} Search Neutral Word Breaker Resources  
 {9E175BA8-F52A-11D8-B9A5-505054503030} Search Null Word Breaker  
 {9E175BA9-F52A-11D8-B9A5-505054503030} Search Gatherer Log File Provider  
 {9E175BB7-F52A-11D8-B9A5-505054503030} Windows Search Service Tripoli Indexer  
 Engine  
 {9E175BB8-F52A-11D8-B9A5-505054503030} Windows Search Service Jet Property  
 Storage Engine  
 {9E358D23-02B2-4CCD-9FEE-6B75EE8DD5CA} PSFactoryBuffer  
 {9E51E0D0-6E0F-11d2-9601-00C04FA31A86}  
 {9E56BE60-C50F-11CF-9A2C-00A0C90A90CE} Mail Service  
 {9E56BE61-C50F-11CF-9A2C-00A0C90A90CE} Desktop Shortcut  
 {9E704F44-90F0-11D1-BA0F-00A0C906B239}  
 {9E77AAC4-35E5-42A1-BDC2-8F3FF399847C} Stream Buffer Sink Segment  
 {9E797ED0-5253-4243-A9B7-BD06C58F8EF3} iTV Playback Feature Segment  
 {9EBB177D-0161-4e2c-81B0-E15D586CFC9F} PSFactoryBuffer  
 {9EC4B4F9-3029-45ad-947B-344DE2A249E2} Urlmon Scheme Handler  
 {9ecb380c-2333-4c68-9691-a569fe446820} MAPISendMailServer  
 {9ecf51f8-cfb1-458d-9485-f5a231afd22f} CLSID\_XMLAutoList  
 {9ED4692C-90F0-11D1-BA0F-00A0C906B239}  
 {9ED96B20-73AA-11D2-952C-0060081840BC} Frame Rate Converter Property Page  
 {9ED96B21-73AA-11D2-952C-0060081840BC} Audio Repackager Property Page  
 {9ED96B22-73AA-11D2-952C-0060081840BC} Dexter Queue  
 {9EFD4CF2-0BAA-350B-9D73-0974077B2F7B}  
 {9F007F18-9C24-4630-8B3E-61F96280C593} Microsoft WBEM Rpc Message Receiver  
 {9F0139EC-2195-42d7-A7B6-41E1DA530AD9} File data caching class  
 {9F36C194-166C-4cbf-B7EA-BF039F950172} PeerGroup Wrapper



## SOFTWARE OUTPUT

{9F377D7E-E551-44f8-9F94-9DB392B03B7B} CProvideWinSATVisuals Class  
 {9F50E8B1-9530-4DDC-825E-1AF81D47AED6} MSVidCtl Analog TV to StreamBufferSource  
 Composition Segment  
 {9F66347C-60C4-4C4D-AB58-D2358685F607}  
 {9F7D7BB5-20B3-11DA-81A5-0030F1642E3C} SettingsEngine Class  
 {9FD4E808-F6E6-4e65-98D3-AA39054C1255} InkRecognizers Class  
 {9FE63AFD-59CF-4419-9775-ABCC3849F861} System Recovery  
 {9ff7242c-364d-425d-95ce-c64f8ee140d1} Mobile Broadband Puk1 Page Class  
 {a015411a-f97d-4ef3-8425-8a38d022aebc} CLSID\_FindExecute  
 {A0227FFC-3AA7-4dc3-9FD7-125745C9EAF6} CameraControl2 Class  
 {A0275511-0E86-4ECA-97C2-ECD8F1221D08} Infrared  
 {A02797fC-C4AE-418C-AF95-E637C7EAD2A1}  
 {A03CD5F0-3045-11CF-8C44-00AA006B6814} IAMExtTransport  
 {a07034fd-6caa-4954-ac3f-97a27216f98a} Query file associations  
 {A08AF898-C2A3-11d1-BE23-00C04FA31009} Windows Mail Envelope  
 {A09C534C-0057-462E-8402-2A21D38BFCA1} New Network category Task  
 {A09CCA86-27BA-4F39-9053-121FA4DC08FC}  
 {A0A7A57B-59B2-4919-A694-ADD0A526C373} Tearless Window Presenter  
 {A0B9B497-AFBC-45AD-A8A6-9B077C40D4F2} Custom Composition Segment from Encoder to  
 Time Shift Sink  
 {a0d018ee-1100-4389-ab44-464faf001288} Authentication UI Logon Sound  
 {A0F93E27-F05D-4153-A151-F3720369A4C7} Microsoft WMI Signed Driver Provider  
 {A1006DE3-2173-11d2-9A7C-00C04FA309D4} CLSID\_COE5Import  
 {a11850eb-4501-4dea-9ef5-1d37f57d247d} Mobile Broadband Create Profile Page Class  
 {A11DB3DC-5FF6-4a0b-AEE6-29BCAC1E11E0}  
 {a1570149-e645-4f43-8b0d-409b061db2fc} EnumBthMtpConnectors Class  
 {A1607060-5D4C-467a-B711-2B59A6F25957} AltTab  
 {A167B942-CD17-4d00-BDD9-8FDC2DC158F2}  
 {a16e1bfff-a80d-48ad-aecd-a35c005685fe} IMA ADPCM ACM Wrapper MFT  
 {A1A2B1C4-0E3A-11D3-9D8E-00C04F72D980} Collection of BDA Tuning Model Component  
 Types(Broadcast Substream Types)  
 {A1F4E726-8CF1-11D1-BF92-0060081ED811} WIA Device Manager  
 {A25821B5-F310-41BD-806F-5864CC441B78} WlanPref LUA  
 {a2a9545d-a0c2-42b4-9708-a0b2badd77c8} Start Menu Pin  
 {A2D75874-6750-4931-94C1-C99D3BC9D0C7} Microsoft Windows Defender  
 {A2D8CFE7-7BA4-4bad-B86B-851376B59134} Windows Parental Controls  
 {A2E3074E-6C3D-11D3-B653-00C04F79498E} BDA Tuner Device Segment  
 {A2E3074F-6C3D-11D3-B653-00C04F79498E}  
 {A2E30750-6C3D-11D3-B653-00C04F79498E} BDA Tuning Model ATSC Tuning Space  
 {A2E6DDA0-06EF-4df3-B7BD-5AA224BB06E8} ImageFile Class  
 {A32552C5-BA61-457A-B59A-A2561E125E33} UPnPDevice Class  
 {A373F500-7A87-11D3-B1C1-00C04F68155C} Windows Search Service Client Side Cache  
 Protocol Handler  
 {a3b3c46c-05d8-429b-bf66-87068b4ce563} Action Center Notification Manager  
 {A3C97737-76D9-4f5f-B917-4DE47FE023C8} CWinsatWMI Class  
 {A3E41207-BE04-492A-AFF0-19E880FF7545} WMI instrumentation:  
 Win32\_ComputerShutdownEvent  
 {A3ECBC41-581A-4476-B693-A63340462D8B} Filter Graph Private Thread

## SOFTWARE OUTPUT

```

{a42c2ccb-67d3-46fa-abe6-7d2f3488c7a3} Windows RTF Previewer
{A45AEC2B-549E-405F-AF3E-C6B03C4FDFBF} ToggleDMRAuthorization
{A470F8CF-A1E8-4f65-8335-227475AA5C46} Encryption Context Menu
{a47401f6-a8a6-40ea-9c29-b8f6026c98b8}
{A47979D2-C419-11D9-A5B4-001185AD2B89} Network List Manager
{A4A1A128-768F-41E0-BF75-E4FDD701CBA} PSFactoryBuffer
{A4B544A1-438D-4B41-9325-869523E2D6C7} TF_CategoryMgr
{a4c31131-ff70-4984-afd6-0609ced53ad6} Shell ChkdskEx Dialog
{A5270F6C-19EC-4E17-9EA1-A7074276B9B9} Windows Search Items Changed Sink
{a542e116-8088-4146-a352-b0d06e7f6af6} Address EditText
{A55803CC-4D53-404c-8557-FD63DBA95D24} WPDShexAutoplay
{a5a3563a-5755-4a6f-854e-afa3230b199f} Library Folder
{A5B020FD-E04B-4e67-B65A-E7DEED25B2CF} TabletManager Class
{A5EFE073-B16F-474f-9F3E-9F8B497A3E08} PSFactoryBuffer
{A6098E79-9C50-4F87-8973-5FB4532C93D8} BTConnectionUi Class
{A6207B2E-7CDD-426A-951E-5E1CBC5AFEAD} PSFactoryBuffer
{a671c915-d95d-4135-b2c3-089356ca694f} Nla Helper Class
{a677570a-2ba2-4e9a-b2e2-8a02cd8b4fd3} CoPrintIsolationHost Class
{a6914418-134b-4bb8-8e3d-7fef7f456caf} CRasDiagHelper Object
{A6A3E580-083F-471b-8F08-87D34F678C95} RDB AutoPlay Handler Class
{A6EE35C6-87EC-47DF-9F22-1D5AAD840C82}
{A6F1684D-AED6-401b-9786-A3E3B53C6641} Parental Controls Control Panel
{a76de978-f3eb-4a4f-9f99-304ad619e2ab} State of OpenSearch view site command
{A7A63E5C-3877-4840-8727-C1EA9D7A4D50} Secure Startup
{A8040703-2640-48B7-96CD-BC8108A4E8F1} SnapinComponent Class
{A82E50BA-8E92-41eb-9DF2-433F50EC2993} MP3 Byte Stream Handler
{A83EF168-CA8D-11D2-B33D-00104BCC4B4A} CLSID_IntProv
{a86ca2f1-af74-4a74-980b-e185d4ca01b0} HomeGroup Task
{A8792A31-F385-493C-A893-40F64EB45F6E} PSFactoryBuffer
{A879E3C4-AF77-44fb-8F37-EBD1487CF920} PSFactoryBuffer
{a8cc4a39-8f83-44eb-a73e-e2848c4f585f} WMPMDE RTSP SINK ACTIVATE
{A8DCF3D5-0780-4EF4-8A83-2CFFAACB8ACE} BDA Tuning Model ATSC Component Type Class
(Broadcast Substream Type)
{A8DFB9A0-8A20-479F-B538-9387C5EEBA2B} VMR Mixer 9
{A8E64375-B645-4314-9EFC-C085981786FA}
{A9397D66-3ED3-11D1-8D99-00C04FC2E0C7}
{A9710FB5-1840-4224-BD42-86831E28E43A} RemMdmObj Class
{A9A33436-678B-4c9c-A211-7CC38785E79D} WinSAT Task Manger Task
{a9ae6c91-1d1b-11d2-b21a-00c04fa357fa} LW Identities
{A9B48EAC-3ED8-11d2-8216-00C04FB687DA} Content Indexer Cleaner
{A9B5F443-FE02-4C19-859D-E9B5C5A1B6C6} Search Gatherer Inline Notification
{A9CF0EAE-901A-4739-A481-E35B73E47F6D} Microsoft DocProp Inplace Edit Box Control
{A9F738C8-6B96-41FA-A155-15ECD67275D0} Windows Search Protocol Handler Search
Connector Creator
{A9FC132B-096D-460B-B7D5-1DB0FAE0C062} RMGetLicense Class
{AA000926-FFBE-11CF-8800-00A0C903B83C} CertServerPolicy Class
{AA10385A-F5AA-4EFF-B3DF-71B701E25E18} Wordpad ODT Document Filter
{AA160628-8775-46e3-837C-F7A2AE66E2F5} Quarantine SoH Protocol processor class

```

## SOFTWARE OUTPUT

```

{aa28fbc7-59f1-4c42-9fd8-ba2be27ea319} Select All command invocation
{AA558FA2-A340-4a23-B765-614BA827CE1D} SppInstallerFactory Class
{AA7E3C50-864C-4604-BC04-8B0B76E637F6}
{AAA288BA-9A4C-45B0-95D7-94D524869DB5} WPDShServiceObj Class
{AABE54D4-6E88-4c46-A6B3-1DF790DD6E0D} Themes tree item callback object for
sysdm.cpl
{AABFB2FA-3E1E-4A8f-8977-5556FB94EA23}
{AAC46A37-9229-4fc0-8CCE-4497569BF4D1} InkRecognizerContext Class
{ab0b37ec-56f6-4a0e-a8fd-7a8bf7c2da96} CLSID_ExplorerHostCreator
{AB2ECE69-56D9-4F28-B525-DE1B0EE44237} PSFactoryBuffer
{AB517586-73CF-489c-8D8C-5AE0EAD0613A} Microsoft DocProp Custom Draw Percent Full
Control
{AB93B6F1-BE76-4185-A488-A9001B105B94} BDEUILauncher Class
{AB944620-79C6-11D1-88F9-0080C7D771BF} Event Publisher
{AB9D6472-752F-43F6-B29E-61207BDA8E06} RDP DShow Video Renderer
{ABB27087-4CE0-4E58-A0CB-E24DF96814BE} InertiaProcessor Class
{ABBA0005-3075-11D6-88A4-00B0D0200F88} ATSCTerrestrial Class
{ABBA0006-3075-11D6-88A4-00B0D0200F88} CDvb Class
{ABBA001B-3075-11D6-88A4-00B0D0200F88} DigitalCable Class
{abd2ad24-f1ff-47ad-82de-3a1edf38e7a1} HomeGroup Task
{ABDBD0B1-7D54-49fb-AB5C-BFF4130004CD} PSFactoryBuffer
{ABE40035-27C3-4A2F-8153-6624471608AF} MSVidCtl Digital TV to StreamBufferSource
Composition Segment
{AC3AC249-E820-4343-A65B-377AC634DC09} WinBio Credential Provider
{AC75D454-9F37-48f8-B972-4E19BC856011}
{AC82FF6D-E524-4c0f-8D0B-0C74C1ECAAEA} InkCursors Class
{ACD453BC-C58A-44D1-BBF5-BFB325BE2D78} Microsoft MPEG-2 Audio Encoder
{ACD857DF-E3D9-36DD-A0AD-7D155D326CE8}
{AD1841CF-0EC5-4b59-ACC4-8329EED299F9}
{AD4C1B00-4BF7-422F-9175-756693D9130D} PSFactoryBuffer
{AD581B00-7B64-4E59-A38D-D2C5BF51DDB3} WindowsMediaLibrarySharingServices Class
{AD6C8934-F31B-4F43-B5E4-0541C1452F6F} WST Pager
{ad763fa6-3b90-41ab-bd44-4f832beee55f} Windows Media Network Source Plugin
{AD8E510D-217F-409B-8076-29C5E73B98E8} Stream Buffer Source
{ad974ae2-e292-4083-a280-0342d68daf55} Updatable Item Set
{ADAB9B51-4CDD-4af0-892C-AB7FA7B3293F} Group Policy Service User Profile
Notification
{adacedf4-9c34-430e-a65f-488f0ab491da}
{ADB880A4-D8FF-11CF-9377-00AA003B7A11}
{ADB880A6-D8FF-11CF-9377-00AA003B7A11} HHCtrl Object
{ADB9F5A4-E73E-49b8-99B6-2FA317EF9DBC} Windows ScreenSaver Properties
{ADBE6DEC-9B04-4A3D-A09C-4BB38EF1351C} XAML Browser Application
{add36aa8-751a-4579-a266-d66f5202ccbb} Print Ordering via the Web
{ADE6444B-C91F-4E37-92A4-5BB430A33340} AppEventsDHTMLConnector 1.0 Object
{ADF95821-DED7-11D2-ACBE-0080C75E246E} Property Setter
{AE03A0A5-DE98-45ff-8016-DDEFF70BCF61} SAL File
{AE054212-3535-4430-83ED-D501AA6680E6} Shell Name Space ListView
{AE1E00AA-3FD5-403C-8A27-2BBDC30CD0E1} Home Networking NAT Traversal via UPnP

```

## SOFTWARE OUTPUT

## Configuration Manager

{ae2079d8-d764-4d79-ab4d-3543847a1a2c}	
{AE62C05D-0A02-30E7-9B51-E9D4DD157207}	
{AE8AFD54-5B57-4961-8A9B-12ADF23B696A}	
{AE9472BF-B0C3-11D2-8D24-00A0C9441E20}	GrfCache Class
{AEB16279-B750-48f1-8586-97956060175A}	MF ASF Property Handler
{AEC17CE3-A514-11D1-AFA6-00AA0024D8B6}	DirectMusicSynthSink
{AEE3E4A8-EF01-4024-A0F1-809D9B096E14}	Windows Media Player Encoder Helper Class
{AEF1693C-839C-4066-82D6-6CC0324C9D20}	Microsoft MPEG-2 Video Encoder Property

## Page

{AF02484C-A0A9-4669-9051-058AB12B9195}	File Save Dialog Legacy
{AF2440F6-8AFC-47d0-9A7F-396A0ACFB43D}	PSFactoryBuffer
{AF2AC6EE-2B16-4756-9475-F319E543EFAA}	SOAPRequest Class
{AF4F6510-F982-11d0-8595-00AA004CD6D8}	Registry Tree Options Utility
{AF604EFE-8897-11D1-B944-00A0C90312E1}	Microsoft Common Browser Architecture
{AF95DC76-16B2-47F4-B3EA-3C31796693E7}	
{AF9F2C0D-6B9F-4e32-A94D-A3E235A31BF7}	XML property store
{AFB40FFD-B609-40A3-9828-F88BBE11E4E3}	Server XML HTTP 3.0
{AFB6C280-2C41-11D3-8A60-0000F81E0E4A}	MPEG-2 Demultiplexer
{AFBA6B42-5692-48EA-8141-DC517DCF0EF1}	Server XML HTTP
{AFD7F94B-1627-436c-80C8-B464AA21CAD3}	WMPlayer SecurityPropPage Class
{b020b123-89b9-46c6-8509-a8bf70447fea}	PSFactoryBuffer
{B0210780-89CD-11d0-AF08-00A0C925CD16}	DirectSoundCapture Object
{B021FF57-A928-459c-9D6C-14DED0C9BED2}	PrinterQueueView Class
{B0395DA5-6A15-4E44-9F36-9A9DC7A2F341}	MMC IconControl class
{b040ea9e-3f5e-48c9-bcdc-304e9d02851f}	CSdGITManager Class
{B056521A-9B10-425E-B616-1FCD828DB3B1}	PSFactoryBuffer
{B084785C-DEE0-4d30-8CA8-05A373E185BE}	NSC Byte Stream Handler
{B091E540-83E3-11CF-A713-0020AFD79762}	File Types Page
{B0A2AB46-F612-4469-BEC4-7AB038BC476C}	WMI High Performance Cooker
{B0A8F3CF-4333-4bab-8873-1CCB1CADA48B}	Drive Type Categorizer
{b0c43320-2315-44a2-b70a-0943a140a8ee}	XPS Signature Manager
{B0D17FC2-7BC4-11d1-BDFA-00C04FA31009}	CLSID_IFontCache
{B0EDF163-910A-11D2-B632-00C04F79498E}	MS TV Video Control
{B106900C-4E8D-4147-8B22-CC60C6B285A8}	Windows Media Player Compositing Mixer
{B12AE898-D056-4378-A844-6D393FE37956}	Windows ThemeUI Pages
{b1325ef5-dd4d-4988-a2b3-c776ad45d0d6}	Authentication UI Legacy Shutdown Dialog
{b155bdf8-02f0-451e-9a26-ae317cfd7779}	delegate folder that appears in Computer
{B196B286-BAB4-101A-B69C-00AA00341D07}	PSFactoryBuffer
{B1EBFC28-C9BD-47A2-8D33-B948769777A7}	
{B210D694-C8DF-490d-9576-9E20CDBC20BD}	Color Calibration Loader
{b27b520e-46db-4720-b9c5-5f80acab23a4}	HomeGroup Task
{b2952b16-0e07-4e5a-b993-58c52cb94cae}	CLSID_DBFolder
{B2A7FD52-301F-4348-B93A-638C6DE49229}	WMPSkinMngr Class
{b2b4fb61-d2dd-4ddd-8001-20f98c6577ef}	Microsoft Query Edit Control
{B2C761C6-29BC-4f19-9251-E6195265BAF1}	Color Management
{B2E8D89A-7A99-4b43-9638-DF4FF83EAC11}	
{B2F2E083-84FE-4a7e-80C3-4B50D10D646E}	Default Category Provider

## SOFTWARE OUTPUT

{B2F3A67C-29DA-4C78-8831-091ED509A475} Microsoft Network Provider  
 {B2F586D4-5558-49D1-A07B-3249DBBB33C2} DirectSoundBufferConfig Object  
 {B323F8E0-2E68-11D0-90EA-00AA0060F86C} StillImage  
 {B32D3949-ED98-4DBB-B347-17A144969BBA} Sync Center Item Properties Extension  
 {B32F4002-BB27-45FF-AF4F-06631C1E8DAD} PSFactoryBuffer  
 {B33F0D7A-1571-4022-B710-D26E9B87DEB8} Autoplay Content Handler  
 {B35EA47E-FA71-34FD-B7E2-EBC050A4FB5A}  
 {B3FD5602-EB0F-415E-9F32-75DA391D6BF9} ExecutivePlatform  
 {B3FF88A4-96EC-4CC1-983F-72BE0EBB368B} Rsop Logging Mode Provider  
 {B401C5EB-8457-427F-84EA-A4D2363364B0} MSVidCtl FilePlayback to Video Renderer  
 Composition Segment  
 {B4124623-FC0E-47CE-BCA9-126A6104ADA1} JournalReader Class  
 {B4B3AECB-DFD6-11d1-9DAA-00805F85CFE3}  
 {B4C8DF59-D16F-4042-80B7-3557A254B7C5} Bluetooth PAN Profile Class Manager  
 {B4D85BBB-D1E6-4F2B-BF43-75CB28500A08} Windows Media Player TunerHelper Class  
 {B4FB3F98-C1EA-428d-A78A-D1F5659CBA93} Other Users Folder  
 {B54E85D9-FE23-499F-8B88-6ACEA713752B}  
 {B5607793-24AC-44c7-82E2-831726AA6CB7} Free Space Categorizer  
 {B5730A90-1A2C-11CF-8C23-00AA006B6814} IAMExtDevice  
 {b5827163-52b0-42c2-940f-f1d72cab1251} WMPMDE NETCHANNEL ACTIVATE  
 {b5866878-bd99-11d0-b04b-00c04fd91550} TypeFactory  
 {B5965ACC-842D-4ABE-A618-9292BB3EE666} MSASR Locale Handler Class (2052)  
 {b5a60a9e-a4c7-4a93-ac6e-0b76d1d87dc4} Device Center Scan Context Menu Extension  
 {B5C8B898-0074-459F-B700-860D4651EA14}  
 {B5EBAFB9-253E-4A72-A744-0762D2685683}  
 {b5f8350b-0548-48b1-a6ee-88bd00b4a5e7} MSAA AccPropServices  
 {B64016F3-C9A2-4066-96F0-BD9563314726} BDA Tuning Model DVB-Satellite Tuning  
 Space  
 {B699E5E8-67FF-4177-88B0-3684A3388BFB} UpdateSearcher Class  
 {B6C292BC-7C88-41EE-8B54-8EC92617E599} WIA Device Manager 2  
 {B708457E-DB61-4C55-A92F-0D4B5E9B1224} MMCViewExt 1.0 Object  
 {b70cc729-28ae-11dd-9676-000000000000} MBN Pin Unblock page  
 {B72F8FD8-0FAB-4dd9-BDBF-245A6CE1485B} QueryParser Class  
 {b75ac000-9bdd-11d0-852c-00c04fd8d503} ADs Access Control Entry Object  
 {B76AD54C-51A2-4230-B516-2CCAA95F8D29} Enable the Desktop Window Manager tree  
 item callback object for sysdm.cpl  
 {b77b1cbf-e827-44a9-a33a-6ccfeeaa142a} ShellItemArray Shell Namespace helper  
 {B77C4C36-0154-4c52-AB49-FAA03837E47F} CLSID\_PublicationServicesServer  
 {B7BBD408-F09C-4aa8-B65E-A00B8FE0F0B9} Windows Theme Preview API  
 {B80AB0A0-7416-11D2-9EEB-006008039E37} MJPEG Compressor  
 {B8558612-DF5E-4F95-BB81-8E910B327FB2} Sync Center (Private)  
 {b85ea052-9bdd-11d0-852c-00c04fd8d503} ADs Access Control List Object  
 {B87BEB7B-8D29-423F-AE4D-6582C10175AC} Video Mixing Renderer  
 {B890AF56-AC8C-11D1-8CB7-00C04FC3261D} CLBTDDispenser Class  
 {b8967f85-58ae-4f46-9fb2-5d7904798f4b} Property System  
 {B9162A23-45F9-47CC-80F5-FE0FE9B9E1A2} Bidi Spooler APIs  
 {b91a4db4-3630-11dc-9eaa-00161718cf63} Burn command invocation  
 {B92E345D-F52D-41F3-B562-081BC772E3B9}

## SOFTWARE OUTPUT

```

{b958f73c-9bdd-11d0-852c-00c04fd8d503} ADS Security Descriptor Object
{B977CB2D-EC6E-4A8F-BFFE-D18682BB0D52} IShareMediaSettingsWriter
{b9815375-5d7f-4ce2-9245-c9d4da436930} CLSID_PreviewEmail
{B98A2BEA-7D42-4558-8BD1-832F41BAC6FD} Backup And Restore
{B9931692-A2B3-4FAB-BF33-9EC6F9FB96AC} TF_LangBarItemMgr
{b9b61a03-caa7-43bb-b859-acd26d73b3f7} CLSID_ResultHandlerFactory
{B9E84FFD-AD3C-40A4-B835-0882EBCBAAA8} UPnPDevices Class
{BA126AD1-2166-11D1-B1D0-00805FC1270E} Network Connection Manager Class
{BA126AD2-2166-11D1-B1D0-00805FC1270E} Network Connection Manager Connection
Enumerator Class
{BA126AD3-2166-11D1-B1D0-00805FC1270E} LAN Connection Manager Class
{BA126AD4-2166-11D1-B1D0-00805FC1270E} LAN Connection Manager Connection
Enumerator Class
{BA126AD5-2166-11D1-B1D0-00805FC1270E} WAN Connection Manager Class
{BA126AD6-2166-11D1-B1D0-00805FC1270E} WAN Connection Manager Connection
Enumerator Class
{BA126AD7-2166-11D1-B1D0-00805FC1270E} Dial-up Connection Class
{BA126AD8-2166-11D1-B1D0-00805FC1270E} Network Group Policies for NLA Class
{BA126AD9-2166-11D1-B1D0-00805FC1270E} Inbound Connection Class
{BA126ADB-2166-11D1-B1D0-00805FC1270E} LAN Connection Class
{BA126ADD-2166-11D1-B1D0-00805FC1270E} Inbound Connection Manager Class
{BA126ADE-2166-11D1-B1D0-00805FC1270E} Inbound Connection Manager Connection
Enumerator Class
{BA126ADF-2166-11D1-B1D0-00805FC1270E} Network Install Queue
{BA126AE0-2166-11D1-B1D0-00805FC1270E} Shared Access Connection Manager
{BA126AE1-2166-11D1-B1D0-00805FC1270E} Shared Access Connection Manager
Enumerated Connection
{BA126AE2-2166-11D1-B1D0-00805FC1270E} Shared Access Connection
{BA126AE3-2166-11D1-B1D0-00805FC1270E} Home Networking Connections Utility Class
{BA126AE5-2166-11D1-B1D0-00805FC1270E} Network Connection Manager Class 2
{BA126E01-2166-11D1-B1D0-00805FC1270E} Connection Manager LUA Inproc Object
{BA126F01-2166-11D1-B1D0-00805FC1270E} Connection Manager LUA Host Object
{BA677074-762C-444b-94C8-8C83F93F6605} User hive background upload task handler
{BA7C0D29-81CA-4901-B450-634E20BB8C34} CPrintTicket WoW Services
{ba818ce5-b55f-443f-ad39-2fe89be6191f} Function Instance Collection Class
{BAA94581-C092-425C-B4D3-7B5EE0BAC3C4} Windows Media Player WMEncProfile2 Class
{BAEA8DC9-45F5-4DF8-A27F-2A277D524B15} WIA Extension Host for 64 bit extensions
{BB07BACD-CD56-4E63-A8FF-CBF0355FB9F4} EventSystem.EventObjectChange2
{BB18C7A0-2186-4be0-97D8-04847B628E02} WpcProviderSupport Class
{BB2D41DF-7E34-4F06-8F51-007C9CAD36BE} WlanAdhoc LUA
{BB44391D-6ABD-422f-9E2E-385C9DFF51FC} DxtCompositor Class
{BB530C63-D9DF-4B49-9439-63453962E598} Encoder Feature Segment
{BB64F8A7-BEE7-4E1A-AB8D-7D8273F7FDB6} Action Center CPL
{bb6df56b-cace-11dc-9992-0019b93a3a84} Background Intelligent Transfer Control
Class 4.0
{BB847B8A-054A-11d2-A894-0000F8084F96} CLSID_IPropFindRequest
{BB89EB37-081E-4F5D-BA35-8D636BB47440} MSASR Locale Handler Class (1028)
{bbb5d0e2-6f4b-4c31-8744-22d0029c4b40} Function Discovery Print Provider

```

## SOFTWARE OUTPUT

{BBC40082-8ABB-4DDD-B1C6-4EE0A9A5DB52}	WMPlayer PlaylistPropPage Class
{BBEC4F81-C2BC-43a7-BD95-9738EE9B6CCA}	WMPlayer DVDPropPage Class
{bbeea841-0a63-4f52-a7ab-a9b3a84ed38a}	MP3 Decoder DMO
{BC08386A-9952-40CD-BA50-9541D64A4B4E}	PSFactoryBuffer
{BC271022-28CD-468A-BBB0-EF7091D8625E}	Connecting Progress Page Class
{BC29A660-30E3-11D0-9E69-00C04FD7C15B}	WDM Streaming VPE Property Set Interface
Handler	
{BC48B32F-5910-47F5-8570-5074A8A5636A}	Sync Results Delegate Folder
{BCA2CD56-422C-44F8-B3F4-A1B7885AC007}	EnumSTSWORDEDIT Class
{BCDE0395-E52F-467C-8E3D-C4579291692E}	MMDeviceEnumerator class
{BD0D38E4-74C8-4904-9B5A-269F8E9994E9}	ImageProcess Class
{BD4F77B3-70B0-4464-83A5-785F205B823B}	InkTablet Class
{BD6EDFCA-2890-482F-B233-8D7339A1CF8D}	
{BD70C020-2D24-11D0-9110-00004C752752}	
{BD7A2E7B-21CB-41b2-A086-B309680C6B7E}	@%systemroot%\system32\mssvp.dll,-112
{bde9ee7c-329f-4fcf-ba7a-f8c6e9b4579d}	DUI Shell View Frame
{BDF23680-C1E5-11D2-9EF7-006008039E37}	Pin Property
{BDFEE05A-4418-11DD-90ED-001C257CCFF1}	Mbn ConnectionProfile Manager
{BDFEE05B-4418-11DD-90ED-001C257CCFF1}	Mbn Interface Manager
{BDFEE05C-4418-11DD-90ED-001C257CCFF1}	Mbn Connection Manager
{BE09F473-7FEB-11d2-9962-00C04FA309D4}	CLSID_MigrateMessageStore
{BE122A0E-4503-11DA-8BDE-F66BAD1E3F3A}	Windows Anytime Upgrade
{BE8E0170-72DC-11D2-952A-0060081840BC}	Stretch Property Page
{BF27441E-CDCE-4659-AEBE-06F6E069714E}	Screen Capture Filter Task Page
{bf29a3a2-d2bf-4a22-96cc-9aceb0f94cba}	Policy for Glass tree item callback object
for sysdm.cpl	
{bf50b68e-29b8-4386-ae9c-9734d5117cd5}	IShellFolder marshaler app compat stub
{BF5CB148-7C77-4d8a-A53E-D81C70CF743C}	AD RMS Rights Policy Template Management
(Manual) Task Handler	
{bf641d1c-29fd-4721-b3b8-48d92d35f7df}	CLSID_QueryFactoryWithOptions
{BF87B6E0-8C27-11D0-B3F0-00AA003761C5}	Capture Graph Builder
{BF87B6E1-8C27-11D0-B3F0-00AA003761C5}	Capture Graph Builder 2
{BF981FDD-B743-11D1-A69A-00C04FB9988E}	MachineSettings Class
{BFCB2C6D-04AA-4fb9-BC72-58E1AF64BE39}	Nap Server Management class
{BFD468D2-D0A0-4bdc-878C-E69C2F5B435D}	CLSID_PreviewUrl
{BFD6C433-4B17-4F6D-A93C-B03FCC4E586E}	WPD PnP Association Manager Class
{BFE18E9C-6D87-4450-B37C-E02F0B373803}	AutomaticUpdates Class
{C01B9BA0-BEA7-41BA-B604-D0A36F469133}	SystemInformation Class
{C03E8500-781E-49a1-8190-CE902D0B2CE7}	Connection to work options Page
{C03E8511-781E-49a1-8190-CE902D0B2CE7}	RAS Dialup CTI Hook Page (non-UI)
{C03E8512-781E-49a1-8190-CE902D0B2CE7}	Dialup CTI Connection Retry Page
{C03E8513-781E-49a1-8190-CE902D0B2CE7}	RAS Dialup Connection Info Page
{C03E8521-781E-49a1-8190-CE902D0B2CE7}	RAS Dialup CTW Hook Page (non-UI)
{C03E8522-781E-49a1-8190-CE902D0B2CE7}	Dialup CTW Connection Retry Page
{C03E8523-781E-49a1-8190-CE902D0B2CE7}	RAS Dialup (CTW) Connection Info Page
{C03E8524-781E-49a1-8190-CE902D0B2CE7}	RAS Dialup (CTW) User Info Page
{C03E8531-781E-49a1-8190-CE902D0B2CE7}	RAS VPN Check Internet Connection
{C03E8532-781E-49a1-8190-CE902D0B2CE7}	RAS VPN Hook Page (non-UI)

## SOFTWARE OUTPUT

```

{C03E8533-781E-49a1-8190-CE902D0B2CE7} RAS VPN Connection Info Page
{C03E8534-781E-49a1-8190-CE902D0B2CE7} RAS VPN User Info Page
{C03E8541-781E-49a1-8190-CE902D0B2CE7} RAS PPPoE Hook Page (non-UI)
{C03E8542-781E-49a1-8190-CE902D0B2CE7} RAS PPPoE Connection Info Page
{C03E8551-781E-49a1-8190-CE902D0B2CE7} Incoming Connection Check Devices Page
{C03E8552-781E-49a1-8190-CE902D0B2CE7} RAS Incoming Connection Hook Page (non-UI)
{C03E8553-781E-49a1-8190-CE902D0B2CE7} Incoming Connection Users Page
{C03E8554-781E-49a1-8190-CE902D0B2CE7} Incoming Connection Devices Page
{C03E8555-781E-49a1-8190-CE902D0B2CE7} Incoming Connection Network Page
{C03E8556-781E-49a1-8190-CE902D0B2CE7} Incoming Connection Save Page
{C03E8557-781E-49a1-8190-CE902D0B2CE7} Incoming Connection Summary Page
{C03E8561-781E-49a1-8190-CE902D0B2CE7} RAS New Connections Page
{C03E8565-781E-49a1-8190-CE902D0B2CE7} RAS Connection To Work Testing Page Class
{C03E8566-781E-49a1-8190-CE902D0B2CE7} RAS Connection To Internet Testing Page
Class
{C03E8568-781E-49a1-8190-CE902D0B2CE7} RAS Connection To Work Finish Page Class
{C03E8569-781E-49a1-8190-CE902D0B2CE7} RAS Connection To Internet Finish Page
Class
{C03E8571-781E-49a1-8190-CE902D0B2CE7} VANUI RAS Connect Page Class
{C03E8572-781E-49a1-8190-CE902D0B2CE7} VANUI RAS Disconnect Page Class
{C03E8581-781E-49a1-8190-CE902D0B2CE7} Set up a new connection
{C03E8582-781E-49a1-8190-CE902D0B2CE7} Set up a new virtual network connection
(VPN)
{C03E8583-781E-49a1-8190-CE902D0B2CE7} Set up a new dialup connection
{C03E8584-781E-49a1-8190-CE902D0B2CE7} Set up a new dialup connection (Internet)
{C03E8585-781E-49a1-8190-CE902D0B2CE7} Set up a new broadband connection
{C03E8586-781E-49a1-8190-CE902D0B2CE7} Incoming Connections Task Class
{C03E8591-781E-49A1-8190-CE902D0B2CE7} XWizard Factory Generated Class
{C03E8592-781E-49A1-8190-CE902D0B2CE7} XWizard Factory Generated Class
{c047c5a9-c407-4a1e-ad7f-11d0861344b7} L2Sec Helper Class
{c04b329e-5823-4415-9c93-ba44688947b0}
{C04D65CF-B70D-11D0-B188-00AA0038C969} Multi Language String
{C0A4145B-E627-40E3-AECC-FD392DC9B959} XWizard Factory Generated Class
{C0B35746-EBF5-11D8-BBE9-505054503030} PSFactoryBuffer
{C0B3C446-3032-4016-926F-9BAE48BEBFBE} IMOfferRA Class
{C0B4E2F3-BA21-4773-8DBA-335EC946EB8B} File Save Dialog
{C0BC4B4A-A406-4EFC-932F-B8546B8100CC} UPnPServices Class
{C0E13E61-0CC6-11d1-BBB6-0060978B2AE6} Data Driven Cleaner
{C100BE9A-D33A-4a4b-BF23-BBEF4663D017} WCN Discovery Provider Class
{C100BEA3-D33A-4a4b-BF23-BBEF4663D017} WCN Discovery Object
{C100BEB7-D33A-4a4b-BF23-BBEF4663D017} WCN Autorun Handler
{C100BEBB-D33A-4a4b-BF23-BBEF4663D017} WCN Elevation Helper
{C100BEBE-D33A-4a4b-BF23-BBEF4663D017}
{C100BED0-D33A-4a4b-BF23-BBEF4663D017}
{C100BED1-D33A-4a4b-BF23-BBEF4663D017}
{C100BED3-D33A-4a4b-BF23-BBEF4663D017}
{C100BED4-D33A-4a4b-BF23-BBEF4663D017}
{C100BED7-D33A-4a4b-BF23-BBEF4663D017}

```



## SOFTWARE OUTPUT

{C100BED9-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEDA-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEDB-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEDC-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEDD-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEDE-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEE1-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEE2-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEE3-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEE5-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEE6-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEE7-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEE9-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEEA-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEEB-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEEC-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEED-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEEE-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEF0-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEF1-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEF2-D33A-4a4b-BF23-BBEF4663D017}  
 {C100BEF3-D33A-4a4b-BF23-BBEF4663D017}  
 {C10B4771-4DA0-11D2-A2F5-00C04F86FB7D} Winmgmt MOF Compiler  
 {C120DE80-FDE4-49f5-A713-E902EF062B8A} MF MP3 Property Handler  
 {c1243ca0-bf96-11cd-b579-08002b30bfeb} Plain Text filter  
 {C1282A7B-9455-48dc-BBBB-46C2EB525AF5} WMPlayer VizResolutionPropPage Class  
 {c15e6bf0-6351-4588-ac4f-ef7d5ec8c16e} WMPlayer LibraryPropPage Class  
 {C169CC11-1EC1-4847-9C0D-D2F2D80D07CF} Microsoft WBEM Smart Object Marshaler  
 {C19FBD0E-7663-44ea-8265-74130671A1D6} OpenSearch Description Location Creator  
 {C1F400A0-3F08-11D3-9F0B-006008039E37} Sample Grabber  
 {C1F400A4-3F08-11D3-9F0B-006008039E37} Null Renderer  
 {c1f85ef8-bcc2-4606-bb39-70c523715eb3} ScheduledDiagnosticCustomHandler  
 {C20447FC-EC60-475E-813F-D2B0A6DECEFE} Extensible Eventing Service  
 {c206f324-bb45-4765-93ff-3bca7306ff2e} CommonLayoutDefinition  
 {C20CE506-5DA9-4B9C-9662-D88BD30E10A1} PrinterQueueViewJobExtension Class  
 {C228A457-53F5-4a76-8035-DF2DA33E76C8}  
 {C2566514-DD44-4c6c-AAAD-FBD2F18D8DEE} Property Set Storage In Memory Object  
 {c278aba7-cc1c-4717-bdfb-db2bca78246e} Grouping Helper Class  
 {C2796011-81BA-4148-8FCA-C6643245113F} Network Tray SSO  
 {c2d2c3a4-9a7e-11da-8bf7-0007e95ead8d} SBF File  
 {C2DAE44D-C850-425c-B466-D8CBC1469F5D}  
 {C2E88C2F-6F5B-4AAA-894B-55C847AD3A2D} WindowsUpdateAgentInfo Class  
 {C2FBB630-2971-11d1-A18C-00C04FD75D13} Microsoft CopyTo Service  
 {C2FBB631-2971-11d1-A18C-00C04FD75D13} Microsoft MoveTo Service  
 {c3278e90-bea7-11cd-b579-08002b30bfeb} Null filter  
 {C3701884-B39B-11D1-9D68-00C04FC30DF6} OleInstall Class  
 {C39E156D-F621-48CF-B0EE-9C47C430543B} Windows Media Player  
 WMEncFileTransferSourcePropertyPage Class

## SOFTWARE OUTPUT

{C4050BC4-29E1-4c8f-BF6E-6EBAD21E0673} HomeGroup Printer Monitor  
 {C40FBD00-88B9-11d2-84AD-00C04FA31A86}  
 {C424F25A-6774-48BC-9F1E-02CCA8C1BE62} Troubleshooting Control Panel  
 {C447080C-D0C3-48AE-B31E-BB3E93591C69} WMEnc DV Timecode Reader  
 {C45268A2-FA81-4E19-B1E3-72EDBD60AEDA} MSVidCtl Enhanced Video Renderer(DX10)  
 Segment  
 {c463a0fc-794f-4fd9-9201-01938ceacafa} RasMobilityManager  
 {C47195EC-CD7A-11D1-8EA3-00C04F9900D7} SysColorCtrl class  
 {c472004d-44fb-41e9-ac0a-7b920384a850} Device Center Print Commands Extension  
 {C47A41B7-B729-424f-9AF9-5CB3934F2DFA} WinSAT Query OEM Customization Object  
 {C49E32C6-BC8B-11d2-85D4-00105A1F8304} Windows Management Instrumentation Backup  
 and Recovery  
 {c4bbbedb4-e9b9-4e41-8fe1-0786480a2173} CL2TPDiagHelper Object  
 {C4BF2784-AE00-41BA-9828-9C953BD3C54A} MSVidCtl CC to Video Renderer Composition  
 Segment  
 {C4C4C481-0049-4E2B-98FB-9537F6CE516D} Encrypt  
 {C4C4C482-0049-4E2B-98FB-9537F6CE516D} Decrypt  
 {C4C4C483-0049-4E2B-98FB-9537F6CE516D} Properties  
 {C4C4C491-0049-4E2B-98FB-9537F6CE516D} Tags  
 {C4C4C492-0049-4E2B-98FB-9537F6CE516D} Tags  
 {C4C4C493-0049-4E2B-98FB-9537F6CE516D} Tags  
 {C4C4C4F1-0049-4E2B-98FB-9537F6CE516D} Encrypt/Tag  
 {C4C4C4F2-0049-4E2B-98FB-9537F6CE516D} Decrypt/Tag  
 {C4C4C4F3-0049-4E2B-98FB-9537F6CE516D} XDS Codec  
 {C4C4C4FC-0049-4E2B-98FB-9537F6CE516D}  
 {C4D81942-0607-11D2-A392-00E0291F3959} Big Switch  
 {C4D81943-0607-11D2-A392-00E0291F3959} Smart Recompressor  
 {C4EC38BD-4E9E-4b5e-935A-D1BFF237D980} Explorer Travel Band  
 {c51b83e5-9edd-4250-b45a-da672ee3c70e} Restore Default Libraries Command  
 {C529C7EF-A3AF-45F2-8A47-767B33AA5CC0} Network Diagnostics Framework  
 {C52FF1FD-EB6C-42CF-9140-83DEFECA7E29} InkObjectXP Class  
 {C531D9FD-9685-4028-8B68-6E1232079F1E} BDA Tuning Model DVB Cable Locator  
 {C5599E1B-FC7B-4883-9FF4-581BBAEF8DBA} Bluetooth FD Provider Proxy  
 {C5702CCC-9B79-11D3-B654-00C04F79498E} Input Devices Collection Class  
 {C5702CCD-9B79-11D3-B654-00C04F79498E} Output Devices Collection Class  
 {C5702CCE-9B79-11D3-B654-00C04F79498E} Video Renderers Collection Class  
 {C5702CCF-9B79-11D3-B654-00C04F79498E} Audio Renderers Collection Class  
 {C5702CD0-9B79-11D3-B654-00C04F79498E} Features Collection Class  
 {C5702CD6-9B79-11D3-B654-00C04F79498E} Custom Composition Segment from Legacy  
 Analog Tv Tuner Device Segment to Data Services Feature Segment  
 {c57a6066-66a3-4d91-9eb9-41532179f0a5} AppSuggestedLocations  
 {C58C4893-3BE0-4B45-A8B5-A63E4B8C8651} Troubleshooting  
 {c5a40261-cd64-4ccf-84cb-c394da41d590} Video Thumbnail Extractor  
 {C5B19592-145E-11d3-9F04-006008039E37} DxtKey Class  
 {C5B56EA1-5853-3310-B3E2-924E9F0BA355}  
 {C5C5C5F0-3ABC-11D6-B25B-00C04FA0C026} XDSToRat Class  
 {C5C5C5F1-3ABC-11D6-B25B-00C04FA0C026} EvalRat Class  
 {C605507B-9613-4756-9C07-E0D74321CB1E} CLSID\_HomeGroupCtrl

## SOFTWARE OUTPUT

```

{C61BFCDF-2E0F-4AAD-A8D7-E06BAFEBCDFE}
{C624BA95-FBCB-4409-8C03-8CCEEC533EF1} UPnPService Class
{c63382be-7933-48d0-9ac8-85fb46be2fdd} Default Folder Menu
{C647B5C0-157C-11D0-BD23-00A0C911CE86} AVI mux Property Page
{C64B9B66-E53D-4c56-B9AE-FEDE4EE95DB1} Condition History Class
{C666E115-BB62-4027-A113-82D643FE2D99} MPEG-2 Sections and Tables
{C68411EA-1396-48f3-AF98-B7F657E35C20} Autoplay Device Handler
{C6B14B32-76AA-4A86-A7AC-5C79AAF58DA7} BDA Tuning Model DVB Tuning Space
{C6B400E2-20A7-4E58-A2FE-24619682CE6C} Microsoft AC3 Encoder
{C6B5F214-0743-3868-B1EA-C4C23CE2AF52}
{C6CC49B0-CE17-11D0-8833-00A0C903B83C} CertGetConfig Class
{C6E13343-30AC-11D0-A18C-00A0C9118956} IAMVideoCompression
{C6E13344-30AC-11D0-A18C-00A0C9118956} IAMDroppedFrames
{C6E13350-30AC-11D0-A18C-00A0C9118956} IAMAnalogVideoDecoder
{C6E13360-30AC-11D0-A18C-00A0C9118956} IAMVideoProcAmp
{C6E13370-30AC-11D0-A18C-00A0C9118956} IAMCameraControl
{C707F6A6-A1F3-45d7-99AA-A2B9491E84AD} CLSID_PublicationServices
{C71566F2-561E-11D1-AD87-00C04FD8FDFF} Microsoft WBEM Universal Refresher
{C72BE2EC-8E90-452c-B29A-AB8FF1C071FC} FunctionDiscovery Class
{c73f6f30-97a0-4ad1-a08f-540d4e9bc7b9} CLSID_AutoListPropertyStore
{c79d1575-b8c6-4862-a284-788836518b97} Windows Display Settings
{C7B6C04A-CBB5-11d0-BB4C-00C04FC2F410} IndexServer Simple Command Creator
{C7CA6167-2F46-4C4C-98B2-C92591368971} New Library Menu Handler
{c827f149-55c1-4d28-935e-57e47caed973} Shell Web Wizard Host Object
{C8B522CF-5CF3-11CE-ADE5-00AA0044773D} Microsoft OLE DB Error Collection Service
{c8b522d0-5cf3-11ce-ade5-00aa0044773d} Microsoft OLE DB Root Enumerator
{c8b522d1-5cf3-11ce-ade5-00aa0044773d} Microsoft OLE DB Data Conversion Library
{c8c97725-c948-4720-bf0f-e3c2273bfb7d} Library Initialization Handler
{c8e6f269-b90a-4053-a3be-499afcec98c4} User Account Control Check Provider
{C90250F3-4D7D-4991-9B69-A5C5BC1C2AE6} PSFactoryBuffer
{c9298eef-69dd-4cdd-b153-bdbc38486781} State of verb Empty Recycle Bin
{C96401CC-0E17-11D3-885B-00C04F72C717} Folder
{C96401CF-0E17-11D3-885B-00C04F72C717} OCX
{C96401D1-0E17-11D3-885B-00C04F72C717} HTML
{C9A14CDA-C339-460B-9078-D4DEBCFABE91}
{C9D849E0-FBF6-4C26-B1EC-B5D5B4E3F29D} Microsoft MPEG-2 Audio Encoder Property
Page
{C9F5FE02-F851-4EB5-99EE-AD602AF1E619} StreamBufferSource
{CA22F5B1-E06F-4A2B-94FC-21E87FE53781} GameUpdateTask Class
{CA2AF3B4-C15E-412b-B453-557746675FB7} WmiPerf Instance Provider
{ca34fe0a-5722-43ad-af23-05f7650257dd} ADPCM ACM Wrapper MFT
{CA38D8DA-C75D-11D1-8F99-00600895E7D5} Interface Proxy Stub
{CA38D8DB-C75D-11D1-8F99-00600895E7D5} Interface Proxy Stub
{CA3FDCA2-BFBE-4eed-90D7-0CAEF0A1BDA1} PSFactoryBuffer
{CA81B096-1D6F-4635-956E-F08C0B2EC342} Windows Media Player WMEncImageSource
Class
{CAAFDD83-CEFC-4E3D-BA03-175F17A24F91} Stream Buffer Recording Control Object
{CACAF262-9370-4615-A13B-9F5539DA4C0A}

```

## SOFTWARE OUTPUT

```

{CAE80521-F685-11d1-AF32-00C04FA31B90} CLSID_OENote
{CB0FC8E5-686A-478B-A252-FDEC8E167B7} scanprofilemgr class
{CB17E772-E1CC-4633-8450-5617AF577905}
{CB1B7F8C-C50A-4176-B604-9E24DEE8D4D1} Getting Started
{CB1DFE3A-EDFF-4d1f-867D-8ADB02926F4B} OpenSearch Description Create Search
Connector Verb Handler
{CB2F6723-AB3A-11d2-9C40-00C04FA30A3E} Microsoft Common Language Runtime Meta
Data
{CB39A782-E5E4-11D1-8CC0-00C04FC3261D} RegDBCompensator Class
{CB46E850-FC2F-11D2-B126-00805FC73204} PSFactoryBuffer
{CB8555CC-9128-11D1-AD9B-00C04FD8FDFF} WbemAdministrativeLocator Class
{CB8C13E4-62B5-4C96-A48B-6BA6ACE39C76}
{cba9e78b-49a3-49ea-93d4-6bcba8c4de07} Mpeg43 Decoder DMO
{CBC84B69-69EA-439B-B791-DF15F60333CF} Biometrics navigate target object
{CBD30858-AF45-11D2-B6D6-00C04FBBDE6E} TV: Pluggable Protocol
{CBD51D89-C22E-4388-A553-FFE638C76E36}
{CC1101F2-79DC-11D2-8CE6-00A0C9441E20} MediaLocator Class
{CC19079B-8272-4D73-BB70-CDB533527B61} HNetCfg.FwProducts
{CC23F537-18D4-4ECE-93BD-207A84726979} MSVidCtl FilePlayback to Audio Renderer
Composition Segment
{CC48A47F-EFD6-4925-A515-28C40C5A78B6} MSASR Locale Handler Class (1041)
{CC58E280-8AA1-11D1-B3F1-00AA003761C5} Smart Tee Filter
{CC58E281-8AA1-11D1-B3F1-00AA003761C5} DirectX Transform Wrapper
{cc5bbec3-db4a-4bed-828d-08d78ee3e1ed} JScript Compact Profile (ECMA 327)
{CC6EEFFB-43F6-46c5-9619-51D571967F7D} Web Publishing Wizard
{CC785860-B2CA-11CE-8D2B-0000E202599C} MPEG Audio Decoder Property Page
{CC7BFB42-F175-11d1-A392-00E0291F3959} Video Effect (1 input) Class Manager
{CC7BFB43-F175-11d1-A392-00E0291F3959} Video Effect (2 input) Class Manager
{CC829A2F-3365-463F-AF13-81DBB6F3A555} BDA Tuning Model Channel ID Tuning Space
{CC9072AB-C000-49D8-A5AA-00266C8DBB9B} Microsoft WBEM _IwbemEnumMarshaling
Enumerator Helper
{CCAA63AC-1057-4778-AE92-1206AB9ACEE6} StreamBufferRecordingAttributes
{CCB4EC60-B9DC-11D1-AC80-00A0C9034873} PDPO Class
{CCDEDADE-AE23-47f3-A588-B09A05CA1A00} DcpSearchTargetServices
{CCFB7955-B4DC-42CE-893D-884D72DD6B19} Biometrics navigate target object
{CD12A3CE-9C42-11D2-BEED-0060082F2054} ClientNetManager Class
{CD184336-9128-11D1-AD9B-00C04FD8FDFF} WbemAuthenticatedLocator Class
{CD1ABFC8-6C5E-4A8D-B90B-2A3B153B886D} Microsoft WBEM
_IWbemConfigureRefreshingSvc Configure Refreshing Services Factory
{cd3aa379-93f4-421b-9802-aeab68b06771} RdpVideoSink Class
{CD3AFA70-B84F-48F0-9393-7EDC34128127} APPLICATION__X_MPLAYER2 Moniker Class
{CD3AFA71-B84F-48F0-9393-7EDC34128127} APPLICATION__X_MS_WMZ Moniker Class
{CD3AFA72-B84F-48F0-9393-7EDC34128127} AUDIO__AIFF Moniker Class
{CD3AFA73-B84F-48F0-9393-7EDC34128127} AUDIO__BASIC Moniker Class
{CD3AFA74-B84F-48F0-9393-7EDC34128127} AUDIO__MID Moniker Class
{CD3AFA76-B84F-48F0-9393-7EDC34128127} AUDIO__MP3 Moniker Class
{CD3AFA77-B84F-48F0-9393-7EDC34128127} AUDIO__MPEG Moniker Class
{CD3AFA78-B84F-48F0-9393-7EDC34128127} AUDIO__MPEGURL Moniker Class

```

## SOFTWARE OUTPUT

{CD3AFA7A-B84F-48F0-9393-7EDC34128127} AUDIO\_\_SCPLS Moniker Class  
 {CD3AFA7B-B84F-48F0-9393-7EDC34128127} AUDIO\_\_WAV Moniker Class  
 {CD3AFA7C-B84F-48F0-9393-7EDC34128127} AUDIO\_\_MP4 Moniker Class  
 {CD3AFA7D-B84F-48F0-9393-7EDC34128127} AUDIO\_\_VND\_DLNA\_ADTS Moniker Class  
 {CD3AFA83-B84F-48F0-9393-7EDC34128127} AUDIO\_\_X\_MS\_WAX Moniker Class  
 {CD3AFA84-B84F-48F0-9393-7EDC34128127} AUDIO\_\_X\_MS\_WMA Moniker Class  
 {CD3AFA88-B84F-48F0-9393-7EDC34128127} VIDEO\_\_AVI Moniker Class  
 {CD3AFA89-B84F-48F0-9393-7EDC34128127} VIDEO\_\_MPEG Moniker Class  
 {CD3AFA8F-B84F-48F0-9393-7EDC34128127} VIDEO\_\_X\_MS\_ASF Moniker Class  
 {CD3AFA90-B84F-48F0-9393-7EDC34128127} VIDEO\_\_X\_MS\_ASF\_PLUGIN Moniker Class  
 {CD3AFA92-B84F-48F0-9393-7EDC34128127} VIDEO\_\_X\_MS\_WM Moniker Class  
 {CD3AFA93-B84F-48F0-9393-7EDC34128127} VIDEO\_\_X\_MS\_WMX Moniker Class  
 {CD3AFA94-B84F-48F0-9393-7EDC34128127} VIDEO\_\_X\_MS\_WMV Moniker Class  
 {CD3AFA95-B84F-48F0-9393-7EDC34128127} VIDEO\_\_X\_MS\_WVX Moniker Class  
 {CD3AFA96-B84F-48F0-9393-7EDC34128127} APPLICATION\_\_X\_WMPLAYER Moniker Class  
 {CD3AFA97-B84F-48F0-9393-7EDC34128127} AUDIO\_\_3GPP Moniker Class  
 {CD3AFA98-B84F-48F0-9393-7EDC34128127} AUDIO\_\_3GPP2 Moniker Class  
 {CD3AFA99-B84F-48F0-9393-7EDC34128127} VIDEO\_\_MP4 Moniker Class  
 {CD3AFA9A-B84F-48F0-9393-7EDC34128127} VIDEO\_\_QUICKTIME Moniker Class  
 {CD3AFA9B-B84F-48F0-9393-7EDC34128127} AUDIO\_\_VND\_MPEG\_TTS Moniker Class  
 {cd4b7782-eb37-4bfe-b9ce-685f634a08dc} CSdWhcNotifier Class  
 {CD5096A1-E7E7-4E09-8B12-CBF2790A87CF} Bluetooth Personal Area Connection

## Enumerator

{CD6C7868-5864-11D0-ABF0-0020AF6B0B7A} CTreeView Control  
 {CDA42200-BD88-11D0-BD4E-00A0C911CE86} Filter Mapper2  
 {CDA8ACB0-8CF5-4F6C-9BA2-5931D40C8CAE} FaxServer Class  
 {CDBD8D00-C193-11D0-BD4E-00A0C911CE86} CMediaPropertyBag  
 {CDBEC9C0-7A68-11D1-88F9-0080C7D771BF} Event Class  
 {cdc32574-7521-4124-90c3-8d5605a34933} Windows Media Player Burn Audio CD Handler  
 {CDC82860-468D-4d4e-B7E7-C298FF23AB2C} ShellItemArray Shell Namespace helper  
 {CE39D6F3-DAB7-41b3-9F7D-BD1CC4E92399} WCF/COM+ Integration Service Moniker  
 {CE69CC1E-1EC0-4847-9C0D-D2F2D80D07CF} Microsoft WBEM Message Service  
 {ceefea1b-3e29-4ef1-b34c-fec79c4f70af} New Shortcut Wizard  
 {ceff45ee-c862-41de-aee2-a022c81eda92} CLSID\_SeparateSingleProcessExplorerHost  
 {CF1BF3B6-7AD0-4410-996B-C78EAFCD3269} Windows Markup File  
 {CF2CF428-325B-48d3-8CA8-7633E36E5A32} AD RMS Rights Policy Template Management

## (Automated) Task Handler

{CF49D4E0-1115-11CE-B03A-0020AF0BA770} AVI Decompressor  
 {CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA} WbemDefaultPathParser  
 {CF67796C-F57F-45f8-92FB-AD698826C602} .contact shell context menu  
 {cfb16474-0a2e-48dc-88ce-8c0adb7e5e46} Windows Media Player Device Options

## Property Page

{cfbc05bc-1b9e-4693-a49c-4e7181d69e0a} Windows Update Control Panel  
 {CFC399AF-D876-11D0-9C10-00C04FC99C8E} Msxml  
 {CFCCC7A0-A282-11D1-9082-006008059382} Darwin App Publisher  
 {CFF9990B-6414-43F1-A526-14EA5EEAFBDA} Library Share Engine  
 {D02AAC50-027E-11D3-9D8E-00C04F72D980} Collection of all the available BDA Tuning

Model Tuning Space objects on this system

## SOFTWARE OUTPUT

{D032FDC6-3736-4AF0-BE08-6F6E52979BBD} New Network category Status Page  
 {D049B20C-5DD0-44FE-B0B3-8F92C8E6D080}  
 {D0565000-9DF4-11D1-A281-00C04FCA0AA7} EventSystem.EventObjectChange  
 {d0b7e02c-e1a3-11dc-81ff-001185ae5e76} DiagnosticProfile  
 {D0E55F9F-0021-42fe-A1DB-C41F5B564EFE} RASMapi Class  
 {D13E3F25-1688-45A0-9743-759EB35CDF9A} AcquisitionManager Class  
 {D1621129-45C4-41AD-A1D1-AF7EAFABEEDC} WIA Default UI  
 {D169C14A-5148-4322-92C8-754FC9D018D8} rtf persistent handler for mapi email  
 {D16B87DE-029E-4C85-92C8-ED8BBC5E882C} Microsoft Embedded Search Gatherer Inline  
 Notification  
 {d1a42999-0adf-11da-b070-0011856571de}  
 {d1a4299a-0adf-11da-b070-0011856571de}  
 {D20EA4E1-3957-11d2-A40B-0C5020524153} Administrative Tools  
 {D215781D-019E-4FA0-903D-0CDCDE13A4F5} Winmgmt MOF Compiler OOP  
 {d23b90d0-144f-46bd-841d-59e4eb19dc59} WMVideo9 Encoder DMO  
 {D2423620-51A0-11D2-9CAF-0060B0EC3D39} XML Parser  
 {D26AA4A5-92AD-48DB-8D59-95EF0DCE6939} CMigrationPlugin Object  
 {D2AC2892-B39B-11D1-8704-00600893B1BD} DirectMusicLoader  
 {D2E0FE7F-D23E-48E1-93C0-6FA8CC346474} UpdateInstaller Class  
 {D2E7041B-2927-42fb-8E9F-7CE93B6DC937} ColorDataProxy  
 {D2ED260C-38F1-4ABE-8B2B-D4A088C54416} PSFactoryBuffer  
 {D31B6A3F-9350-40DE-A3FC-A7EDEB9B7C63} WMI instrumentation:  
 Win32\_SystemConfigurationChangeEvent  
 {d34a6ca6-62c2-4c34-8a7c-14709c1ad938} Common Places FS Folder  
 {D34BD150-6D84-443E-83EE-04C7682377E4} Unsecured Net Connect Control Class  
 {D3588AB0-0781-11CE-B03A-0020AF0BA770} AVI/WAV File Source  
 {D39E7BDD-7D05-46b8-8721-80CF035F57D7} CivicAddress Report Class  
 {D3C536B8-D0EC-48AB-838F-D4CC9A281BB5} STSServerInstance Class  
 {d3c86d56-03a1-42d5-af4c-1b612be90448} CLSID\_TryHarderItemFactory  
 {D4480A50-BA28-11d1-8E75-00C04FA31A86} Add Network Place  
 {d450a8a1-9568-45c7-9c0e-b4f9fb4537bd} Installed Updates  
 {D4692569-5A04-351D-8BA7-5F43AB458DF6}  
 {D4DCD3D7-B4C2-47D9-A6BF-B89BA396A4A3}  
 {d4f01ada-979c-491e-bac3-cd3c0e7bcf82} Online Id Filter  
 {D4F4D30B-0B29-4508-8922-0C5797D42765} WIA Default Segmentation Filter  
 {D51BD5A1-7548-11CF-A520-0080C77EF58A} Wave Parser  
 {D51BD5A2-7548-11CF-A520-0080C77EF58A} MIDI Parser  
 {D51BD5A3-7548-11CF-A520-0080C77EF58A} Multi-file Parser  
 {D51BD5A5-7548-11CF-A520-0080C77EF58A} File stream renderer  
 {D5307D61-F9BC-4de1-94EA-1DEF24DF4BB2}  
 {d54378cd-91d8-4e10-a00b-819f9a9efcb1} CoFilterPipeline Class  
 {D5753BBB-C5A8-4F50-9D81-210BAB0C5FB6} Mpeg-2 Stats  
 {d58960ba-2ef3-4910-9e34-c911b1710180} ShellTravelLog  
 {D5978620-5B9F-11D1-8DD2-00AA004ABD5E} SENS Network Events  
 {D5978630-5B9F-11D1-8DD2-00AA004ABD5E} SENS Logon Events  
 {D5978640-5B9F-11D1-8DD2-00AA004ABD5E} SENS OnNow Events  
 {D5978650-5B9F-11D1-8DD2-00AA004ABD5E} SENS Logon2 Events  
 {D5C66BE1-C209-11d1-8DEC-00C04FC2E0C7}

## SOFTWARE OUTPUT

{D5ED6B03-EDA3-4cbc-9FF1-60182438C8F6} WSD Print Proxy Class  
 {D6015EC3-FA16-4813-9CA1-DA204574F5DA} AlgController Class  
 {D6108DC8-FBAC-426e-8A3C-1BCA926E5805} Enable transparent glass tree item  
 callback object for sysdm.cpl  
 {D63A1416-FCEC-4431-862F-E8056223DD03} Windows Photo Viewer DropTarget  
 {D63A5850-8F16-11CF-9F47-00AA00BF345C} WBEM Framework Instance Provider  
 {D63AA156-D534-4BAC-9BF1-55359CF5EC30} Sync Center User Profile Notification  
 Handler  
 {D6564DE1-6163-3076-A8FB-D301CB439E30}  
 {D66949A0-C766-48D7-B2C6-4A85382BE9C1} MSASR Locale Handler Class (3082)  
 {D66D6F99-CDAA-11D0-B822-00C04FC9B31F} Multi Language ConvertCharset  
 {D6791A63-E7E2-4fee-BF52-5DED8E86E9B8} Portable Devices Menu  
 {D682C4BA-A90A-42FE-B9E1-03109849C423} StreamBufferComposeRecordingObj  
 {D68AF00A-29CB-43FA-8504-CE99A996D9EA} Microsoft WBEM (non)Standard Marshaling  
 for IwbemServices  
 {D6EBC66B-8921-4193-AFDD-A1789FB7FF57} PSFactoryBuffer  
 {D6F8EC75-A388-47de-BA3A-903B12A38E86} PSFactoryBuffer  
 {D6FEDB1D-CF21-4BD9-AF3B-C5468E9C6684} MMCVersionInfo 1.0 Object  
 {D707877E-4D9C-11d2-8784-F6E920524153} User Property Pages  
 {D722AF63-6A0D-4e37-BD40-CF6FAC79A83C} WMPDMCCoreServices Class  
 {D73733C8-CC80-11D0-B225-00C04FB6C2F5} FaxServer Class  
 {D76334CA-D89E-4BAF-86AB-DDB59372AFC2} MSVidCtl CC to Audio Renderer Composition  
 Segment  
 {D7B70EE0-4340-11CF-B063-0020AFC2CD35} DirectDraw Object  
 {D7C1AEB5-10F2-48cb-A182-F7EF79C51B19} WSD Publisher  
 {D8280A4F-FFED-3E98-8928-9F504A4A3361}  
 {D82BE2B0-5764-11D0-A96E-00C04FD705A2} IShellFolderBand  
 {d84fa0c2-b0b3-4470-9345-75db0ec5a83a} Universal Delegate Folder  
 {d851f103-8c90-4321-aff0-58ba5bd421c2} SharedAccess Notification Sink  
 {D8559EB9-20C0-410E-BEDA-7ED416AECC2A} Windows Defender  
 {D8872739-DF50-4ED5-B8A7-F03DCD0DCD5A} PSFactoryBuffer  
 {D8BD090D-3F39-45FD-B29A-7FC62C2E59C3} ExtTransport2 Class  
 {D8BF32A2-05A5-44c3-B3AA-5E80AC7D2576} DrawingAttributes Class  
 {D8F0F5E7-11C5-4E95-BBFF-0F110C0221C4}  
 {d912f8cf-0396-4915-884e-fb425d32943b} Property Helper Object  
 {D9403860-297F-4A49-BF9B-77898150A442}  
 {D94EDF02-EFE5-4F0D-85C8-F5A68B3000B1}  
 {D957171F-4BF9-4de2-BCD5-C70A7CA55836} Interval Class  
 {D969A300-E7FF-11d0-A93B-00A0C90F2719} New Menu Handler  
 {D978F0CB-DEBA-4388-83BE-D3E106E02A4F} CardSpaceIETokenProvider Class  
 {d9b3211d-e57f-4426-aaef-30a806add397} Shell Library API  
 {D9BB4CEE-B87A-47F1-AC92-B08D9C7813FC} BDA Tuning Model Digital Cable Tuning  
 Space  
 {D9F9C262-6231-11D3-8B1D-00C04FB6BD3D} WM ASF Writer Properties  
 {DA4E3DA0-D07D-11d0-BD50-00A0C911CE86} ActiveMovie Filter Categories  
 {DA67B8AD-E81B-4c70-9B91-B417B5E33527} Windows Search Shell Service Object  
 {DAA92564-78C8-40A3-96D2-9115A76B8F29} WPD Settings Completion Page Class  
 {DAC9F469-0C67-4643-9258-87EC128C5941} SREngine Class

## SOFTWARE OUTPUT

{DAFD8210-5711-4B91-9FE3-F75B7AE279BF} DirectSoundGargleDMO  
 {db4f3fa7-5a08-4100-95de-b46df509b902} Legacy View Available Networks Task Class  
 {DB5D1FF4-09D7-11D1-BB10-00C04FC9A3A3} FILEMGMT 1.0 Object  
 {DB5D1FF5-09D7-11D1-BB10-00C04FC9A3A3} SvcVwr 1.0 Object  
 {DBC85A2C-C0DC-4961-B6E2-D28B62C11AD4} GameStatistics Class  
 {DC0C0FE7-0485-4266-B93F-68FBF80ED834} Microsoft DVBC Network Provider  
 {DC1C5A9C-E88A-4dde-A5A1-60F82A20AEF7} File Open Dialog  
 {DC7A02CD-2E47-406C-BA5A-B08EC00C4238} MAPISendMailServer  
 {DC8A3F5A-92B9-4C38-A81F-296612813880}  
 {DC923725-0FDD-45E1-AE74-EA09182E739B} Microsoft WBEM Wbem Token Cache  
 {DCB00C01-570F-4A9B-8D69-199FDBA5723B} NetworkListManager  
 {dcbd6fa8-032f-11d3-b5b1-00c04fc324a1} speechtextservice class  
 {DCED8DB0-11A5-4b16-AB9D-4E28CA38C99F} Advanced Configuration Dialog  
 {DCF33DF4-B510-439F-832A-16B6B514F2A7} Microsoft WBEM \_IWbemRefresherMgr  
 Refresher Cache Factory  
 {DD06A84F-83BD-4d01-8AB9-2389FEA0869E} Dot11 AdHoc Manager  
 {DD313E04-FEFF-11d1-8ECD-0000F87A470C} User Assist  
 {DD522ACC-F821-461A-A407-50B198B896DC} HardwareDeviceNotif  
 {DD732BF4-B9A8-4f46-BA39-F4C010929F5F}  
 {DD75716E-B42E-4978-BB60-1497B92E30C4} text persistent handler for mapi email  
 {DDC0EED2-ADBE-40b6-A217-EDE16A79A0DE} GenericFilter  
 {DDE33513-774E-4BCD-AE79-02F4ADFE62FC}  
 {DDE5783A-88B9-11d2-84AD-00C04FA31A86}  
 {de2d022d-2480-43be-97f0-d1fa2cf98f4f} PropertyKeyCollection Class  
 {DE3F3560-3032-41B4-B6CF-F703B1B95640} Windows Search Service Profile Notify  
 Handler  
 {DE4874D1-FEEE-11d1-A0B0-00C04FA31A86}  
 {DE4874D2-FEEE-11d1-A0B0-00C04FA31A86}  
 {DE75D012-7A65-11D2-8CEA-00A0C9441E20} DxtJpeg Class  
 {DE77BA04-3C92-4d11-A1A5-42352A53E0E3} Home Group Member Status  
 {DE815B00-9460-4F6E-9471-892ED2275EA5} RecoManager Class  
 {DE9C1288-0F09-40ff-BA84-7F19279FA74B} Identity Listener CLSID  
 {DECBDC16-E824-436e-872D-14E8C7BF7D8B} RtpObject Class  
 {DF0B3D60-548F-101B-8E65-08002B2BD119} PSSupportErrorInfo  
 {DF60686C-2941-4893-80C0-F13173B719D3} HomeGroup State  
 {DFA14C43-F385-4170-99CC-1B7765FA0E4A} WpcNotificationsMonitor  
 {DFD74844-990B-4410-9DA0-2848EFA85D14} WMPPlayer ClipPropPage Class  
 {DFFACDC5-679F-4156-8947-C5C76BC0B67F} delegate folder that appears in Users  
 Files Folder  
 {E03E85B0-7BE3-4000-BA98-6C13DE9FA486} ConditionFactory Class  
 {E05592E4-C0B5-11D0-A439-00A0C9223196} Plug In Distributor: IKsQualityForwarder  
 {e0ca5340-4534-11cf-b952-00aa0051fe20} HTML filter  
 {E0CBC546-8950-43DD-99A9-A418DB7DD0B5} Could Not Connect Page Class  
 {E0F158E1-CB04-11d0-BD4E-00A0C911CE86} WaveOut and DSound Class Manager  
 {E0FA581D-2188-11D2-A739-00C04FA377A1} Provider Binder for DS OLE DB Provider  
 {E10A508F-1699-40ba-A0DD-9DEB2D4DCAC3}  
 {E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E} PSIProfileNotify  
 {E137B0D0-7A93-11D2-8CEA-00A0C9441E20} DxtJpegPP Class



## SOFTWARE OUTPUT

{E13EF4E4-D2F2-11d0-9816-00C04FD91972} Menu Site  
 {E16C0593-128F-11D1-97E4-00C04FB9618A} Simple File-based Log  
 {E16C0594-128F-11D1-97E4-00C04FB9618A} ARIES Log Recovery Engine  
 {E18AF75A-08AF-11D3-B64A-00C04F79498E} Custom Composition Segment from Legacy  
 Analog Tv Tuner Device Segment to Standard Video Renderer Device Segment  
 {E1BA41AD-4A1D-418F-AABA-3D1196B423D3} SDChangeObj Class  
 {E1C5D730-7E97-4D8A-9E42-BBAE87C2059F} DeviceManager Class  
 {E1D0AB13-2FE6-4DF0-8917-ED80CF0FEF6B}  
 {E1DE74AD-C368-4104-ADB1-57D00577247A} WLAN Media Manager  
 {E1F1A0B8-BEEE-490D-BA7C-066C40B5E2B9} Microsoft DTV-DVD Audio Decoder  
 {E2085F28-FEB7-404A-B8E7-E659BDEAAA02} UPnPDeviceFinder Class  
 {E20870E2-3AD1-4b64-87BE-5AD5F17A53F0} rtf persistent handler for mapi email  
 {E211B736-43FD-11D1-9EFB-0000F8757FCD}  
 {e2183960-9d58-4e9c-878a-4acc06ca564a} Microsoft DocProp Custom Draw Multi-Value  
 Property Control  
 {E23CE3EB-5608-4E83-BCEF-27B1987E51D7}  
 {E2448508-95DA-4205-9A27-7EC81E723B1A} SBE2 Sink  
 {E2510970-F137-11CE-8B67-00AA00A3F1A6} AVI mux  
 {E26B366D-F998-43ce-836F-CB6D904432B0} RealTimeStylus Class  
 {E2A4E630-7AD8-44f0-B6EE-D36EA4C6EB94} Network Diagnostics Client Interface  
 Wrapper  
 {e2b07466-5250-4fc2-8949-46bf91f8cad0}  
 {E2C6779C-B7DE-3311-8A5B-41922461E7C0}  
 {E2CBCB87-9C07-4523-A78F-061499C83987} WMI instrumentation:  
 Win32\_VolumeChangeEvent  
 {e2fb4720-f45f-4a3c-8cb2-2060e12425c3} MF AVI Property Handler  
 {E302CB55-5F9D-41A3-9EF3-61827FB8B46D} PSFactoryBuffer  
 {E30629D1-27E5-11CE-875D-00608CB78066} Audio Renderer  
 {E30629D2-27E5-11CE-875D-00608CB78066} Audio Capture Filter  
 {E3633C03-DF7A-41E0-B903-CC349A05E021} PSFactoryBuffer  
 {E37A73F8-FB01-43dc-914E-AAEE76095AB9} WTVFile Property Handler  
 {E37E2028-CE1A-4f42-AF05-6CEABC4E5D75} Shell Icon Handler for Application  
 References  
 {E37EF07F-8266-448B-8059-C2B35BAFE0CF} SnapinState Class  
 {e3a4e5ca-55b2-4a06-b1ab-8fbec7bca4b} Authentication UI Terminal Services Bump  
 Dialog  
 {E3D5D93C-1663-4A78-A1A7-22375DFEBAEE} InkTransform Class  
 {e3e478d6-a2f2-4791-89a3-21f5c78dc3ec} File enumerator helper  
 {E413D040-6788-4C22-957E-175D1C513A34} Sync Center Conflict Delegate Folder  
 {E4206432-01A1-4BEE-B3E1-3702C8EDC574} Line 21 Decoder 2  
 {E423AF7C-FC2D-11d2-B126-00805FC73204} RemoteHelper Class  
 {E436EBB1-524F-11CE-9F53-0020AF0BA770} System Clock  
 {E436EBB2-524F-11CE-9F53-0020AF0BA770} Filter Mapper  
 {E436EBB3-524F-11CE-9F53-0020AF0BA770} Filter Graph  
 {E436EBB5-524F-11CE-9F53-0020AF0BA770} File Source (Async.)  
 {E436EBB6-524F-11CE-9F53-0020AF0BA770} File Source (URL)  
 {E436EBB7-524F-11CE-9F53-0020AF0BA770} IPersistMoniker Plug In Distributor  
 {E436EBB8-524F-11CE-9F53-0020AF0BA770} Filter Graph no thread

## SOFTWARE OUTPUT

```

{E44E5D18-0652-4508-A4E2-8A090067BCB0} Default Programs command object for Start
menu
{e44e9428-bdbc-4987-a099-40dc8fd255e7} Execute Unknown
{e46787a1-4629-4423-a693-be1f003b2742} MF WAV Property Handler
{E474E05A-AB65-4f6a-827C-218B1BAAF31F} MF Video Mixer
{e4796550-df61-448b-9193-13fc1341b163} Property Store
{E4979309-7A32-495E-8A92-7B014AAD4961} VMR ImageSync 9
{E4BCAC13-7F99-4908-9A8E-74E3BF24B6E1} DirectSoundCapture 8.0 Object
{E573236F-55B1-4EDA-81EA-9F65DB0290D3}
{E598560B-28D5-46aa-A14A-8A3BEA34B576} Windows Photo Viewer Video Verbs
{E5B4EAA0-B2CA-11CE-8D2B-0000E202599C} MPEG Video Decoder Property Page
{E5B8E079-EE6D-4E33-A438-C87F2E959254} Location Class
{E5CA59F5-57C4-4DD8-9BD6-1DEEEDD27AF4} Microsoft InkEdit Control
{E5CB7A31-7512-11D2-89CE-0080C792E5D8} Microsoft Common Language Runtime Meta
Data
{e60687f7-01a1-40aa-86ac-db1cbf673334} SUSInternal Class 1.0
{E63DE750-3BD7-4BE5-9C84-6B4281988C44} Windows Search Scope Rule
{E6442437-6C68-4f52-94DD-2CFED267EFB9} CLSID_TrayDesktopBand
{E64CCC22-8E66-4822-9F2F-7FC385645A03}
{E69FD98D-7EBE-4C01-BFED-67B4E4616A49} Browser Thread Handshake
{E70C92A9-4BFD-11d1-8A95-00C04FB951F3} CLSID_StoreNamespace
{e74e57b0-6c6d-44d5-9cda-fb2df5ed7435} CCertProvider
{e755468c-02f5-4d96-8487-3be68ffe633a} Elevated Object Factory Server Manager
{e760e244-abb3-4c3c-b925-0781c8ceb46c}
{E77026B0-B97F-4cbb-B7FB-F4F03AD69F11} Tuning Model Xml Serialization Utility
{E7772804-3287-418E-9072-CF2B47238981}
{E77CC89B-7401-4c04-8CED-149DB35ADD04} WindowsParentalControls Class
{E77E1B8B-ECF3-4af0-8B5E-EB13739D5344}
{E785DD9D-3F87-3679-BB58-A3A4C80F4256}
{E7B2FB72-D728-49B3-A5F2-18EBF5F1349E} PSFactoryBuffer
{E7DE9B1A-7533-4556-9484-B26FB486475E} Network Map
{e7ed314f-2816-4c26-aeb5-54a34d02404c} KernelCeipCustomHandler
{E810CEE7-6E51-4cb0-AA3A-0B985B70DAF7} StrokeBuilder Class
{E8140D53-6535-46a5-B8A1-DA6C571DA9B9} Quarantine SoH Protocol constructor class
{E8167EE2-AB45-4BAA-BD03-12590436D789} CLSID_COE7Import
{e82a2d71-5b2f-43a0-97b8-81be15854de8} ShellLink for Application References
{E846F0A0-D367-11D1-8286-00A0C9231C29}
{E882F102-F626-49E9-BD68-CE2BE7E59EA0} SoundRecorder WAV Dest
{E882F102-F626-49E9-BD68-CE2BE7E59EB0} SoundRecorder Volume Watch
{E882F102-F626-49E9-BD68-CE2BE7E59EC0} SoundRecorder Null Renderer
{E9495B87-D950-4ab5-87A5-FF6D70BF3E90} Security Center
{E96767E0-7EAA-45e1-8E7D-64414AFF281A} File Prop Sheet Page Helper
{E96F5460-09CE-4f46-88B1-F4B6B4A8E252} Windows Media Player Transcode Files Cache
Cleanup Handler
{E974D26D-3D9B-4D47-88CC-3872F2DC3585} XPS Object Factory
{E9A6AB1B-0C9C-44AC-966E-560C2771D1E8} DrawAttrsXP Class
{E9F4EBAB-D97B-463e-A2B1-C54EE3F9414D} Net Scheme Handler
{EA022610-0748-4c24-B229-6C507EBDFDBB} CLSID_HomeGroupCtrlServer

```

## SOFTWARE OUTPUT

```

{EA2C6B24-C590-457B-BAC8-4A0F9B13B5B8} User Account Control Settings
{EA30C654-C62C-441f-AC00-95F9A196782C} GestureRecognizer Class
{EA502722-A23D-11D1-A7D3-0000F87571E3} Group Policy Object
{EA678830-235D-11d2-A8B6-0000F8084F96} CLSID_IPropPatchRequest
{ea72d00e-4960-42fa-ba92-7792a7944c1d} Run as different user context menu handler
{EA7BAE70-FB3B-11CD-A903-00AA00510EA3}
{EA7BAE71-FB3B-11CD-A903-00AA00510EA3}
{ea8b451c-5a19-49cf-bc5e-98accca49ef3} Library Factory
{EA9155A3-8A39-40b4-8963-D3C761B18371} PerfTrack TaskHandler class
{ea9a0595-056e-4d74-980f-bb53f6bb9f8d} PSFactoryBuffer
{EAC8A024-21E2-4523-AD73-A71A0AA2F56A} WbemQuery
{eb124705-128b-40d4-8dd8-d93ed12589a4} WPL property store
{eb4d075a-65c0-476b-956c-c605eade03f7} DemuxRender
{EB56EAE8-BA51-11d2-B121-00805FC73204}
{EB6B4457-F013-4E5A-9B05-1D44E4D6FAEB} HomeGroup Sharing Hosted Listener
{EB87E1BD-3233-11D2-AEC9-00C04FB68820} WbemStatusCode
{EBB08C45-6C4A-4FDC-AE53-4EB8C4C7DB8E} TF_LangBarMgr
{EC00BA63-C73A-4679-AC8D-69366C766989} SBE Stats - receiver side
{EC529B00-1A1F-11D1-BAD9-00609744111A} WDM Streaming VPE VBI Property Set
Interface Handler
{ecabafaa-7f19-11d2-978e-0000f8757e2a} Activity Property Unmarshal Class
{ecabafab-7f19-11d2-978e-0000f8757e2a} SecurityEnvoy
{ecabafac-7f19-11d2-978e-0000f8757e2a} Transaction Property Unmarshal Class
{ecabafad-7f19-11d2-978e-0000f8757e2a} NonRootTransactionEnvoy
{ecabafae-7f19-11d2-978e-0000f8757e2a} sca Class
{ecabafaf-7f19-11d2-978e-0000f8757e2a} ClassFactory Activator Class
{ecabafb0-7f19-11d2-978e-0000f8757e2a} obja Class
{ecabafb1-7f19-11d2-978e-0000f8757e2a} stapa Class
{ecabafb2-7f19-11d2-978e-0000f8757e2a} vca Class
{ecabafb3-7f19-11d2-978e-0000f8757e2a} User Context Object
{ecabafb4-7f19-11d2-978e-0000f8757e2a} User Context Properties Association Object
{ecabafb5-7f19-11d2-978e-0000f8757e2a} PoolMgr Class
{ecabafb6-7f19-11d2-978e-0000f8757e2a} Object Pool Activator Class
{ecabafb7-7f19-11d2-978e-0000f8757e2a} Contruction Activator Class
{ecabafb9-7f19-11d2-978e-0000f8757e2a} COM+ Instance Tracking Component
{ecabafbc-7f19-11d2-978e-0000f8757e2a} COM+ Event Notification Server
{ecabafc0-7f19-11d2-978e-0000f8757e2a} cfw Class
{ecabafc2-7f19-11d2-978e-0000f8757e2a} Queued Components Recorder
{ecabafc3-7f19-11d2-978e-0000f8757e2a} QC Listener Class
{ecabafc4-7f19-11d2-978e-0000f8757e2a} Queued Components Player
{ecabafc6-7f19-11d2-978e-0000f8757e2a} New Moniker
{ecabafc7-7f19-11d2-978e-0000f8757e2a} Queue Moniker
{ecabafc9-7f19-11d2-978e-0000f8757e2a} QC Queue Administration Class
{ecabafca-7f19-11d2-978e-0000f8757e2a} COM+ QC Dead Letter Queue Listener Starter
{ecabafcb-7f19-11d2-978e-0000f8757e2a} QC Marshal Interceptor Class
{ecabafcc-7f19-11d2-978e-0000f8757e2a} Partition Property Unmarshal Class
{ecabafcd-7f19-11d2-978e-0000f8757e2a} Tracking Info Collection Unmarshal Class
{ecabafce-7f19-11d2-978e-0000f8757e2a} Tracking Info Object Unmarshal Class

```

## SOFTWARE OUTPUT

```

{ecabafcf-7f19-11d2-978e-0000f8757e2a} EventRegistrar Class
{ecabafd0-7f19-11d2-978e-0000f8757e2a} Soap Activator Class
{ecabafd3-7f19-11d2-978e-0000f8757e2a} ObjWrapperMarshaler Class
{ecabb0a8-7f19-11d2-978e-0000f8757e2a} COM+ Services GetSecurityCallContext
{ecabb0aa-7f19-11d2-978e-0000f8757e2a} Byot Server Extended Object
{ecabb0ab-7f19-11d2-978e-0000f8757e2a} MTSEvents Class
{ecabb0ac-7f19-11d2-978e-0000f8757e2a} MTSLocator Class
{ecabb0bd-7f19-11d2-978e-0000f8757e2a} CrmClerk Class
{ecabb0be-7f19-11d2-978e-0000f8757e2a} CrmRecoveryClerk Class
{ecabb0bf-7f19-11d2-978e-0000f8757e2a} MessageMover Class
{ecabb0c0-7f19-11d2-978e-0000f8757e2a} DispenserManager
{ECABB0C3-7F19-11D2-978E-0000F8757E2A} ComEvents.ComServiceEvents
{ecabb0c4-7f19-11d2-978e-0000f8757e2a} Debug Dump Server
{ecabb0c5-7f19-11d2-978e-0000f8757e2a} Partition Moniker
{ECABB0C6-7F19-11D2-978E-0000F8757E2A} ComEvents.ComSystemAppEventData
{ecabb0c7-7f19-11d2-978e-0000f8757e2a} SOAP Moniker
{ecabb0c8-7f19-11d2-978e-0000f8757e2a} CServiceConfig Class
{ECABB0C9-7F19-11D2-978E-0000F8757E2A}
{ECABB0CA-7F19-11D2-978E-0000F8757E2A}
{ECD32AEA-746F-4dcB-BF68-082757FAFF18} DynamicRenderer Class
{ECD4FC4D-521C-11D0-B792-00A0C90312E1} Shell Rebar BandSite
{ECD4FC4E-521C-11D0-B792-00A0C90312E1} Shell Band Site Menu
{ECD4FC4F-521C-11D0-B792-00A0C90312E1} Menu Desk Bar
{ECE71064-011D-45b7-AEF2-3B626985E937} CPropertyObject Class
{ECF03A32-103D-11d2-854D-006008059367} MyDocs Drop Target
{ecf5bf46-e3b6-449a-b56b-43f58f867814} Identity Store Profile Notification
{ed1d0fdf-4414-470a-a56d-cfb68623fc58} Play with Windows Media Player
{ED228FDF-9EA8-4870-83b1-96b02CFE0D52} Games Explorer
{ed50fc29-b964-48a9-afb3-15ebb9b97f36} printhood delegate folder
{ed6ae9cf-ad35-46b7-ac30-3f8b9eb5349f} TryHarderFactory
{ED7BA470-8E54-465E-825C-99712043E01C} All Tasks
{ED81C073-1F84-4ca8-A161-183C776BC651} Lat/Long Report Class
{ED8C108E-4349-11D2-91A4-00C04F7969E8} XML HTTP Request
{ED999FF5-223A-4052-8ECE-0B10C8DBAA39} ActualWbemUnauthenticatedLocator Class
{edb5f444-cb8d-445a-a523-ec5ab6ea33c7} Share Manager
{EDD36029-D753-4862-AA5B-5BCCAD2A4D29} Property Store Collection
{edd749de-2ef1-4a80-98d1-81f20e6df58e} PLAP Logon Provider Filter
{EDF6970E-4557-4BC5-86C2-C7E52A06B27F} PSFactoryBuffer
{EE09B103-97E0-11CF-978F-00A02463E06F} Scripting.Dictionary
{ee2e9ce0-0fe1-4eea-8f30-e4728b56f183} Category Drop Target
{EE366069-1832-420F-B381-0479AD066F19}
{EE4DA6A4-8C52-4a63-BBB8-97C93D7E1B6C} APPLICATION__X_MS_WMD Moniker Class
{EE8E4870-A889-4DC4-969F-F38F707F4AC2} CTaskCondition
{eea0c191-dda8-4656-8fc4-72bdeba8a78} Library Property Store
{EEBEACC0-D281-4557-A0F4-B2193F86B1EA} Net Connect Page Class
{EEC5DCCA-05DC-4B46-8AF7-2881C1635AEA}
System.ServiceModel.Internal.TransactionBridge
{EEC6993A-B3FD-11D2-A916-00C04FB98638} Microsoft USB PID Class Driver

```

## SOFTWARE OUTPUT

{eec97550-47a9-11cf-b952-00aa0051fe20} HTML File persistent handler  
 {EF011F79-4000-406D-87AF-BFFB3FC39D57} DirectSoundCompressorDMO  
 {EF114C90-CD1D-484E-96E5-09CFAF912A21} DirectSoundDistortionDMO  
 {ef1c0450-0b48-4384-94ae-d1cb35641f86} Categorizer Factory  
 {EF3E932C-D40B-4F51-8CCF-3F98F1B29D5D} DirectSoundEchoDMO  
 {ef43ecfe-2ab9-4632-bf21-58909dd177f0} Folder Customization Tab  
 {EF4D1E1A-1C87-4AA8-8934-E68E4367468D} WebCheck  
 {ef5db4c2-9312-422c-9152-411cd9c4dd84} PortableDeviceService Class  
 {EF8AD2D1-AE36-11D1-B2D2-006097DF8C11} Global Folder Settings  
 {EF985E71-D5C7-42D4-BA4D-2D073E2E96F4} DirectSoundI3DL2ReverbDMO  
 {EFA24E64-B078-11D0-89E4-00C04FC9E26E}  
 {EFB4A0CB-A01F-451C-B6B7-56F02F77D76F} GenericRecognizer Class  
 {EFCA3D92-DFD8-4672-A603-7420894BAD98} DirectSoundFlangerDMO  
 {EFE3FA02-45D7-4920-BE96-53FA7F35B0E6} BDA Tuning Model DVB Terrestrial 2 Locator  
 {EFE6629C-81F7-4281-BD91-C9D604A95AF6} DirectSoundChorusDMO  
 {F020E586-5264-11d1-A532-0000F8757D7E}  
 {F0285374-DFF1-11D3-B433-00C04F8ECD78} ConsolePower Class  
 {F0291081-E87C-4E07-97DA-A0A03761E586} Drawing  
 {F02C1A0D-BE21-4350-88B0-7367FC96EF3C} Computers and Devices  
 {F04CC277-03A2-4277-96A9-77967471BDFF} Sync Center Conflict Properties Extension  
 {f07f3920-7b8c-11cf-9be8-00aa004b9986} Microsoft Office Filter  
 {F087771F-D74F-4C1A-BB8A-E16ACA9124EA} Background Intelligent Transfer Control  
 Class 1.5  
 {F08C5AC2-E722-4116-ADB7-CE41B527994B} Bluetooth Authentication Agent SSO  
 {f0ae1542-f497-484b-a175-a20db09144ba}  
 {F1390A9A-A3F4-4E5D-9C5F-98F3BD8D935C} Sync Setup Delegate Folder  
 {F198A89A-5042-4294-ADF1-CB163E549798} Win32\_EncryptableVolumeProvider Class  
 {F1E752C3-FD72-11D0-AEF6-00C04FB6DD2C} DocConfig 1.0 Object  
 {f1f3b524-b27f-4a64-8d26-c654800b79d3} Run Backup AutoPlay Handler Class  
 {F20487CC-FC04-4B1E-863F-D9801796130B} Sync Center Shell Service Object  
 (Internal)  
 {F2102C37-90C3-450C-B3F6-92BE1693BDF2} Windows Security Center ISV API  
 {F22F5E05-585C-4def-8523-6555CFBC0CB3} CTocEntry  
 {f235ce7d-b143-4d4f-ad93-64e48d53a5fb} CLSID\_KnownAutoListManager  
 {F2472B49-5214-4D3A-A662-04F09250D694} WlanDlgNonUIFinishPage Class  
 {f26a669a-bcbb-4e37-abf9-7325da15f931} AutoPlayVerb  
 {f270c64a-ffb8-4ae4-85fe-3a75e5347966} ADs Security Utility Object  
 {f2c3faae-c8ac-11d0-bcdb-00c04fd8d5b6} DsPropertyPages.OU  
 {F31091EA-B0A8-11D6-B6FC-005056C00008} CmiFactory Class  
 {F3130CDB-AA52-4C3A-AB32-85FFC23AF9C1} Microsoft WBEM New Event Subsystem  
 {F3364BA0-65B9-11CE-A9BA-00AA004AE837} Shell File System Folder  
 {F3368374-CF19-11d0-B93D-00A0C90312e1} OrderListExport  
 {f371728a-6052-4d47-827c-d039335dfe0a} Mpeg4 Decoder DMO  
 {F37AFD4F-E736-4980-8650-A486B1F2DF25} Windows\_Search\_OutlookToolbar  
 {F37C5810-4D3F-11d0-B4BF-00AA00BBB723} Security Shell Extension  
 {F382DA49-9148-4a22-AF78-C378DFC32D02} MS\_InstalledGameProv Class  
 {F3BDFAD3-F276-49e9-9B17-C474F48F0764} CQueryWinSAT Class  
 {F3C633A2-46C8-498E-8FBB-CC6F721BBCDE}

## SOFTWARE OUTPUT

{f3cc4ca3-22c2-40ec-ac3c-89d8a43373b0}	Include the selected folder in a library.
{f3d06e7c-1e45-4a26-847e-f9fcdee59be0}	Copy as Path Menu
{f4086d4e-2e05-428b-92de-87d8d0bb4262}	Pnrp Helper Class
{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}	JScript Language
{f414c261-6ac0-11cf-b6d1-00aa00bbbb58}	JScript Language Authoring
{f414c262-6ac0-11cf-b6d1-00aa00bbbb58}	JScript Language Encoding
{f447b69e-1884-4a7e-8055-346f74d6edb3}	Resampler DMO
{F46316E4-FB1B-46eb-AEDF-9520BFBB916A}	Dynamic Storage Object
{F4655419-DAF2-42ab-9178-3B6AC903170C}	RNWF MSM Helper Class
{f4be747e-45c4-4701-90f1-d49d9ac30248}	PerfCenter Enabler
{F5078F19-C551-11D3-89B9-0000F81FE221}	XML Parser
{F5078F27-C551-11D3-89B9-0000F81FE221}	
{F5078F31-C551-11D3-89B9-0000F81FE221}	XML Parser 3.0
{F5078F32-C551-11D3-89B9-0000F81FE221}	XML DOM Document 3.0
{F5078F33-C551-11D3-89B9-0000F81FE221}	Free Threaded XML DOM Document 3.0
{F5078F34-C551-11D3-89B9-0000F81FE221}	XML Schema Cache 3.0
{F5078F35-C551-11D3-89B9-0000F81FE221}	XML HTTP 3.0
{F5078F36-C551-11D3-89B9-0000F81FE221}	XSL Template 3.0
{F5078F37-C551-11D3-89B9-0000F81FE221}	
{F5078F39-C551-11D3-89B9-0000F81FE221}	XML Data Source Object 3.0
{F5078F3F-C551-11D3-89B9-0000F81FE221}	XML Moniker 3.0
{F5078F40-C551-11D3-89B9-0000F81FE221}	XML Document 3.0
{F5078F41-C551-11D3-89B9-0000F81FE221}	XML Island 3.0
{f507f854-308b-401e-a1b7-b55ba6ba679a}	Association Property Handler
{F562A2C8-E850-4F05-8E7A-E7192E4E6C23}	PSFactoryBuffer
{F56F6FDD-AA9D-4618-A949-C1B91AF43B1A}	Action Center Shell Service Object
{F5A55D36-8750-432C-AB52-AD49A016EABC}	Microsoft WMI Provider Subsystem Binding

Factory

{F5B63656-069D-4E80-B4FD-9E0DB16604D8}	
{f5d121ed-c8ac-11d0-bcdb-00c04fd8d5b6}	DsPropertyPages.User
{f5d121ee-c8ac-11d0-bcdb-00c04fd8d5b6}	DsPropertyPages.Group
{f5d121ef-c8ac-11d0-bcdb-00c04fd8d5b6}	DsPropertyPages.Domain
{f5d121f0-c8ac-11d0-bcdb-00c04fd8d5b6}	DsPropertyPages.Contact
{f5d121f3-c8ac-11d0-bcdb-00c04fd8d5b6}	DsPropertyPages.Volume
{f5d121f4-c8ac-11d0-bcdb-00c04fd8d5b6}	DsPropertyPages.Computer
{F5D3E63B-CB0F-4628-A478-6D8244BE36B1}	
{F5F75737-2843-4F22-933D-C76A97CDA62F}	Microsoft WMI Provider Subsystem Decoupled

Basic Event Provider

{f60163ce-2b8d-458d-ab2c-40f215767514}	CLSID_IndexScopeFiller
{F6166DAD-D3BE-4ebd-8419-9B5EAD8D0EC7}	ShellItemArray Shell Namespace helper
{F618C514-DFB8-11D1-A2CF-00805FC79235}	Catalog2 Class
{F61FFEC1-754F-11d0-80CA-00AA005B4383}	BandProxy
{F62D062C-4732-44D2-BD62-124B8AE1657C}	WMPlayer PluginsPropPage Class
{F6B96EDA-1A94-4476-A85F-4D3DC7B39C3F}	DvbSiParser Class
{F6BEC032-233E-4B58-BEE9-DE13942BF136}	PSFactoryBuffer
{F6D90F11-9C73-11D3-B32E-00C04F990BB4}	XML DOM Document
{F6D90F12-9C73-11D3-B32E-00C04F990BB4}	Free Threaded XML DOM Document
{F6D90F14-9C73-11D3-B32E-00C04F990BB4}	XML Data Source Object

## SOFTWARE OUTPUT

```

{F6D90F16-9C73-11D3-B32E-00C04F990BB4} XML HTTP
{f713df56-e581-482c-9453-3e934eac5899}
{F72A76A0-EB0A-11D0-ACE4-0000C0CC16BA} KsDataTypeHandlerVideo2
{F72A76E0-EB0A-11D0-ACE4-0000C0CC16BA} KsDataTypeHandlerVBI
{f744e496-1b5a-489e-81dc-fbd7ac6298a8} Microsoft PenInputPanel Control
{f77d9c1c-5aff-4341-b028-57f7510aa91c} CLSID_AssociationListExtender
{f792beee-aeaf-4ebb-ab14-8bc5c8c695a8} Media Foundation MP2demux
{F7A4F1DA-96C3-4BCF-BEB3-1D9FFDE89EE9} ComCacheCleanup 1.0 Object
{F7AFD75B-BF8C-4a11-BDB9-04AD66182F84} MF Video Presenter 2
{F7B9271E-46D8-4B6A-B5CF-E6A4F7F49732} Alternates Class
{f7c0039a-4762-488a-b4b3-760ef9a1ba9b} PortableDeviceFTM Class
{f7ffe0a0-a4f5-44b5-949e-15ed2bc66f9d} MSScreen 9 encoder DMO
{F80608CB-5A88-4046-9E4B-3C1BB368F2DA} WMPDMCPlaylist Class
{f81b1b56-7613-4ee4-bc05-1fab5de5c07e} MF MPEG-4 Property Handler
{f81e9010-6ea4-11ce-a7ff-00aa003ca9f6} Shell extensions for sharing
{F82DF8F7-8B9F-442E-A48C-818EA735FF9B} Pen and Touch Control Panel
{F8383852-FCD3-11d1-A6B9-006097DF5BD4} Progress Dialog
{F8388A40-D5BB-11D0-BE5A-0080C706568E} Infinite Pin Tee Filter
{f83cbf45-1c37-4ca1-a78a-28bcb91642ec} CD Audio Burning Hook
{f85d5d94-6851-44f7-bb3a-bfd0949abf1d} Tree property value cache
{F885120E-3789-4fd9-865E-DC9B4A6412D2} IARPUinstallStringLauncher
{f8a56d3e-e304-4a9f-a916-5187019d7759}
{f8b8412b-dea3-4130-b36c-5e8be73106ac} CLSID_PreviewHtml
{F8D253D9-89A4-4daa-87B6-1168369F0B21} UpdateServiceManager Class
{F8FB6E07-55E6-4BB9-96BC-2393A039CEE7} UIGlobalNotify Class
{F90B5F36-367B-402A-9DD1-BC0FD59D8F62}
{F90FE5FE-E88B-4578-9C81-79210FD53D41} Infrastructure Adapter Page Selection
Class
{F91D96C7-8509-4D0B-AB26-A0DD10904BB7} CMpeg2Stream
{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B} Windows Script Host Shell Object
{F935DC26-1CF0-11D0-ADB9-00C04FD58A0B} Windows Script Host Network Object
{F9769A06-7ACA-4E39-9CFB-97BB35F0E77E} BDA Tuning Model Auxiliary Inputs Tuning
Space
{F979439C-48B7-4525-AB0E-EEE06439227A} Windows Media Player
WMEncPrivatePluginConnector Class
{F97B8A60-31AD-11CF-B2DE-00DD01101B85} Stretch
{F9A7AB61-C0BC-490e-A7FE-BFF26B327A3F} OpenSearch Result Context Menu
{F9AE8980-7E52-11d0-8964-00C04FD611D7} MSIDX
{F9AE8981-7E52-11d0-8964-00C04FD611D7} MSIDX ErrorLookup
{f9bcb2f0-7df0-4a39-932e-bdef29dfb16b} Authentication UI Session Control
{F9F4D292-87F5-4E2D-98A1-590391932490} Windows Media Player WMEncBasicEdit Class
{FA10746C-9B63-4b6c-BC49-FC300EA5F256} Enhanced Video Renderer
{FA4B375A-45B4-4D45-8440-263957B11623} Microsoft DVBS Network Provider
{FA5FE7C5-6A1D-4B11-B41F-F959D6C76500} Microsoft MPEG-2 Media Foundation Media
Sink
{FA7C375B-66A7-4280-879D-FD459C84BB02} WebDVD Adminitration class
{FA8A68B2-C864-4BA2-AD53-D3876A87494B} StreamBufferConfig
{FAB24754-0440-439b-A223-B1D360062D1D} Dhcp Quarantine Enforcement Client

```

## SOFTWARE OUTPUT

## Callback Component

{FABD6EA5-AE10-4E7A-B83B-5F07ACC84214} WPD Settings Review Page Class  
 {FAE3D380-FEA4-4623-8C75-C6B61110B681}  
 {FAF53CC4-BD73-4E36-83F1-2B23F46E513E} VssEvent  
 {FB012959-F4F6-44D7-9D09-DAA087A9DB57}  
 {FB40360C-547E-4956-A3B9-D4418859BA66}  
 {fb479c02-9ec4-4fed-8599-debe037452cb} Shell Hardware Mixed Content Handler

## Cancelled

{FB4CDF30-A741-421d-BCFA-6CC530D053FB} Microsoft.SQLLITE.MOBILE.OLEDB.3.0  
 {FB64825E-498C-45E8-ADD4-37E0C4FC68A6} SBE Stats - Mpeg2 Video Stream Analysis  
 {FB74F625-7D25-4455-B840-7B870B5B9322} Windows Media SDK MSB Source Plugin  
 {fbe5c2f7-027e-4033-afcd-faa04af9be8d} Authentication UI Background Dialog  
 {fbeb8a05-beee-4442-804e-409d6c4515e9} ShellFolder for CD Burning  
 {fbeb71b-a592-4880-b096-9429ebe119db} Extensible L2Sec Helper Class  
 {fc1ee10b-7ef6-41b5-bb60-98d26dd9fcd1}  
 {FC220AD8-A72A-4EE8-926E-0B7AD152A020} MXXMLWriter  
 {FC5B8A24-DB05-4A01-8388-22EDF6C2BBBA} Bidi Spooler APIs  
 {FC772AB0-0C7F-11D3-8FF2-00A0C9224CF4} BDA MPEG2 Transport Information Filter  
 {fcc2867c-69ea-4d85-8058-7c214e611c97} Authentication UI Terminal Services Bump

## Dialog Server

{FCC74B77-EC3E-4dd8-A80B-008A702075A9} ARP UninstallString Launcher  
 {fccf70c8-f4d7-4d8b-8c17-cd6715e37fff} Search Control  
 {FCF7A6F2-3300-4386-9A4F-0DD4E3226507} WmiPerf Instance Provider  
 {FD0A5AF3-B41D-11D2-9C95-00C04F7971E0} IBDA\_DeviceControl  
 {FD351EA1-4173-4AF4-821D-80D4AE979048} Stream Buffer V2 Source  
 {FD853CD9-7F86-11d0-8252-00C04FD85AB4} CLSID\_IMimeInternational  
 {FD853CDB-7F86-11d0-8252-00C04FD85AB4} CLSID\_IMimeBody  
 {FD853CDC-7F86-11d0-8252-00C04FD85AB4} CLSID\_IMimeMessageParts  
 {FD853CDD-7F86-11d0-8252-00C04FD85AB4} CLSID\_IMimeAllocator  
 {FD853CDE-7F86-11d0-8252-00C04FD85AB4} CLSID\_IMimeSecurity  
 {FD853CDF-7F86-11d0-8252-00C04FD85AB4} CLSID\_IVirtualStream  
 {FD853CE0-7F86-11d0-8252-00C04FD85AB4} CLSID\_IMimeHeaderTable  
 {FD853CE1-7F86-11d0-8252-00C04FD85AB4} CLSID\_IMimePropertySet  
 {FD853CE2-7F86-11d0-8252-00C04FD85AB4} CLSID\_IMimeMessageTree  
 {FD853CE3-7F86-11d0-8252-00C04FD85AB4} CLSID\_IMimeMessage  
 {FD853CE6-7F86-11d0-8252-00C04FD85AB4} CLSID\_ISMTPTransport  
 {FD853CE7-7F86-11d0-8252-00C04FD85AB4} CLSID\_IPOP3Transport  
 {FD853CE8-7F86-11d0-8252-00C04FD85AB4} CLSID\_INNTPTransport  
 {FD853CE9-7F86-11d0-8252-00C04FD85AB4} CLSID\_IRASTransport  
 {FD853CEA-7F86-11d0-8252-00C04FD85AB4} CLSID\_IRangeList  
 {FD853CEB-7F86-11d0-8252-00C04FD85AB4} CLSID\_IIMAPTransport  
 {FD853CED-7F86-11d0-8252-00C04FD85AB4} CLSID\_IMimePropertySchema  
 {FDD384CC-78C6-4E6D-8694-1DACBEE57F96} PSFactoryBuffer  
 {fe1290f0-cfbd-11cf-a330-00aa00c16e65} @%SystemRoot%\system32\dsquery.dll,-553  
 {FE12CD81-5158-4bd8-A37C-A621BC0E143B}  
 {fe5afc2-e681-4ada-9703-ef39b8ecb9bf} Library Description  
 {fe7c0d2b-27f1-4e97-951b-cf6e165eeab6} TSMFActivate Class  
 {FEA4300C-7959-4147-B26A-2377B9E7A91D} DirectSoundFullDuplex Object



## SOFTWARE OUTPUT

```

{FEB50740-7BEF-11CE-9BD9-0000E202599C} MPEG Video Codec
{FEC52D45-D657-42c3-B43E-BF64B95E7072} WIA Preview Component
{fecd606e-7161-4cbc-a868-4703867823ea} WMDM Transcode Property Page
{FEF10FA2-355E-4e06-9381-9B24D7F7CC88}
{FF036D13-5D4B-46DD-B10F-106693D9FE4F}
{FF151822-B0BF-11D1-A80D-000000000000} Microsoft OLE DB Root Binder for Internet
Publishing
{FF2A742B-CA25-4507-BD93-6BA9B8E8965F} Fat MSM Helper Class
{ff363bfe-4941-4179-a81c-f3f1ca72d820} HomeGroup SSO
{ff48dba4-60ef-4201-aa87-54103eef594e} UIAutomation Client Central Class
{ff8a32e3-a9a7-4093-b9c4-5b5b4f30ab63} CLSID_ResultShape
{ff9e6131-a8c1-4188-aa03-82e9f10a05a8} Elevatable Shortcut
{FFB8655F-81B9-4fce-B89C-9A6BA76D13E7} Shell Execute Hardware Event Handler
{FFCDB781-D71C-4D10-BD5F-0492EAFD90A} PSFactoryBuffer
{ffe1df5f-9f06-46d3-af27-f1fc10d63892} HomeGroup CPL Advanced Settings Writer
{FFE2A43C-56B9-4bf5-9A79-CC6D4285608A} Windows Photo Viewer Image Verbs

```

-----  
cmd\_shell v.20130405

(Software) Gets shell open cmds for various file types

Classes\exefile\shell\open\command

LastWrite Time Tue Jul 14 04:53:38 2009 (UTC)

Cmd: "%1" %\*

Classes\cmdfile\shell\open\command

LastWrite Time Tue Jul 14 04:53:38 2009 (UTC)

Cmd: "%1" %\*

Classes\batfile\shell\open\command

LastWrite Time Tue Jul 14 04:53:38 2009 (UTC)

Cmd: "%1" %\*

Classes\csfile\shell\open\command not found.

Classes\htafile\shell\open\command

LastWrite Time Mon Dec 1 12:56:39 2014 (UTC)

Cmd: C:\Windows\SysWOW64\mshta.exe "%1" %\*

Classes\piffile\shell\open\command

LastWrite Time Tue Jul 14 04:53:38 2009 (UTC)

Cmd: "%1" %\*

Clients\StartMenuInternet\IExplore.exe\shell\open\command

LastWrite Time Mon Dec 1 14:13:22 2014 (UTC)

Cmd: C:\Program Files\Internet Explorer\iexplore.exe

-----  
codeid v.20100608

## SOFTWARE OUTPUT

(Software) Gets CodeIdentifier DefaultLevel value

CodeID

Policies\Microsoft\Windows\Safer\CodeIdentifiers

LastWrite time: Thu Jan 7 21:08:49 2016 Z

-----  
ctrlpn1 v.20100116

(Software) Get Control Panel info from Software hive

Microsoft\Windows\CurrentVersion\Control Panel

Cpls key has no values.

don't load key

hdwwiz.cpl

telephon.cpl

appwiz.cpl

ncpa.cpl

sysdm.cpl

desk.cpl

inetcpl.cpl

joy.cpl

mmsys.cpl

Firewall.cpl

powercfg.cpl

intl.cpl

timedate.cpl

main.cpl

collab.cpl

irprops.cpl

tabletpc.cpl

infocardcpl.cpl

bthprops.cpl

System.ControlPanel.Category [Thu Jan 28 22:39:45 2016 UTC]

Category -1,4

%SystemRoot%\System32\Speech\SpeechUX\sapi.cpl

-----  
defbrowser v.20091116

(Software) Gets default browser setting from HKLM

Default Browser Check #1

Clients\StartMenuInternet

LastWrite Time Fri Jan 1 20:52:18 2016 (UTC)

## SOFTWARE OUTPUT

Default Browser : IEXPLORE.EXE

Default Browser Check #2

Classes\HTTP\shell\open\command

LastWrite Time Mon Dec 1 14:14:02 2014 (UTC)

Default Browser = "C:\Program Files\Internet Explorer\iexplore.exe" %1

-----  
 Launching direct v.20120513

Microsoft

Wow6432Node\Microsoft

Fri Mar 25 02:13:40 2016 DirectDraw\MostRecentApplication - mbam.exe

-----  
 disablesr v.20120914

(Software) Gets the value that turns System Restore either on or off

Microsoft\Windows NT\CurrentVersion\SystemRestore

LastWrite Time Wed Apr 13 11:20:11 2016 (UTC)

DisableSR value not found.

-----  
 drivers32 v.20130408

(Software) Get values from the Drivers32 key

Microsoft\Windows NT\CurrentVersion\Drivers32

LastWrite Time Sun Feb 14 15:57:33 2016 (UTC)

wave3 - wdmaud.drv

aux - wdmaud.drv

aux2 - wdmaud.drv

mixer3 - wdmaud.drv

vidc.i420 - iyuv\_32.dll

msacm.msadpcm - msadp32.acm

VIDC.UYVY - msyuv.dll

midimapper - midimap.dll

mixer1 - wdmaud.drv

midi3 - wdmaud.drv

vidc.mrle - msrle32.dll

mixer2 - wdmaud.drv

VIDC.YUY2 - msyuv.dll

VIDC.YVU9 - tsbyuv.dll

VIDC.IYUV - iyuv\_32.dll

wave - wdmaud.drv

midi1 - wdmaud.drv

aux4 - wdmaud.drv

wave2 - wdmaud.drv

VIDC.VVYU - msyuv.dll

## SOFTWARE OUTPUT

aux1 - wdmaud.drv  
midi4 - wdmaud.drv  
aux3 - wdmaud.drv  
msacm.imaadpcm - imaadp32.acm  
MSVideo8 - VfwWDM32.dll  
midi - wdmaud.drv  
wavemapper - msacm32.drv  
wave4 - wdmaud.drv  
vidc.msvc - msvidc32.dll  
mixer4 - wdmaud.drv  
mixer - wdmaud.drv  
msacm.l3acm - C:\Windows\System32\l3codeca.acm  
midi2 - wdmaud.drv  
msacm.msgsm610 - msgsm32.acm  
wave1 - wdmaud.drv  
msacm.msg711 - msg711.acm

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32  
LastWrite Time Sun Feb 14 15:57:33 2016 (UTC)

vidc.iyuv - iyuv\_32.dll  
wave3 - wdmaud.drv  
aux - wdmaud.drv  
aux2 - wdmaud.drv  
vidc.cvid - iccvid.dll  
mixer3 - wdmaud.drv  
vidc.i420 - iyuv\_32.dll  
vidc.yvu9 - tsbyuv.dll  
msacm.msadpcm - msadp32.acm  
midimapper - midimap.dll  
mixer1 - wdmaud.drv  
midi3 - wdmaud.drv  
vidc.mrle - msrle32.dll  
mixer2 - wdmaud.drv  
vidc.yuy2 - msyuv.dll  
wave - wdmaud.drv  
midi1 - wdmaud.drv  
aux4 - wdmaud.drv  
vidc.uyvy - msyuv.dll  
wave2 - wdmaud.drv  
aux1 - wdmaud.drv  
midi4 - wdmaud.drv  
aux3 - wdmaud.drv  
msacm.imaadpcm - imaadp32.acm  
midi - wdmaud.drv  
wavemapper - msacm32.drv  
vidc.yvyu - msyuv.dll  
wave4 - wdmaud.drv  
vidc.msvc - msvidc32.dll

## SOFTWARE OUTPUT

```

mixer4 - wdmaud.drv
mixer - wdmaud.drv
msacm.l3acm - C:\Windows\SysWOW64\l3codeca.acm
midi2 - wdmaud.drv
msacm.msgsm610 - msgsm32.acm
msacm.msg711 - msg711.acm
wave1 - wdmaud.drv

```

```

-----
drwatson v.20081219
(Software) Gets Dr. Watson settings from Software hive

```

```

Microsoft\Windows NT\CurrentVersion\AeDebug
LastWrite Time Tue Jul 14 04:53:25 2009 (UTC)
Debugging is Disabled

```

```

Microsoft\DrWatson not found.

```

```

Analysis Tips: For Dr. Watson settings information check:
http://www.windowsnetworking.com/kbase/WindowsTips/Windows2000/RegistryTips/Registry
Tools/DrWatson.html

```

```

-----
emdmgmt v.20120207
(Software) Gets contents of EMDMgmt subkeys and values

```

```

EMDMgmt
Microsoft\Windows NT\CurrentVersion\EMDMgmt
LastWrite Time Wed Apr 6 14:25:02 2016 (UTC)

```

```

FreeAgent Drive
  LastWrite: Sat Dec 12 12:39:48 2015 Z
  VSN: F8F8-F3C5
  LastTestedTime: Sat Dec 12 12:39:48 2015 Z

```

```

Recovery image
  LastWrite: Thu Sep 10 17:04:27 2015 Z
  VSN: E2D0-4536

```

```

HP Elitebook
  LastWrite: Thu Sep 10 20:50:45 2015 Z
  VSN: 8CCF-DA80

```

```

System
  LastWrite: Thu Sep 10 20:50:45 2015 Z
  VSN: 4ACF-3B09

```

```

Windows
  LastWrite: Thu Sep 10 17:04:26 2015 Z

```

## SOFTWARE OUTPUT

VSN: 8CCF-DA80

Seagate Backup Plus Drive

LastWrite: Fri Sep 11 15:07:01 2015 Z

VSN: 5C44-3D6F

LastTestedTime: Fri Sep 11 15:07:01 2015 Z

#5&12e35340&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

LastWrite: Wed Sep 23 03:08:14 2015 Z

VSN: 72AD-2013

Disk&Ven\_&Prod\_&Rev\_2.20

LastWrite: Sat Mar 19 22:26:21 2016 Z

SN: 0718011120035AF&0

VSN: BA5D-2061

Disk&Ven\_&Prod\_&Rev\_2.20

LastWrite: Sat Mar 19 22:36:29 2016 Z

SN: 0718011120035AF&0

VSN: 20C7-421F

Disk&Ven\_&Prod\_&Rev\_2.20

LastWrite: Sat Mar 19 22:30:21 2016 Z

SN: 0718011120035AF&0

VSN: 20EC-234B

Disk&Ven\_&Prod\_&Rev\_2.20

LastWrite: Mon Oct 19 13:06:16 2015 Z

SN: 0718011120035AF&0

VSN: 308F-3940

Disk&Ven\_&Prod\_&Rev\_PMAP

LastWrite: Mon Sep 14 18:39:07 2015 Z

SN: 07032B5A180AA664&0

Vol Name: SMALLBLACK

VSN: F86E-7DF0

Disk&Ven\_&Prod\_&Rev\_PMAP

LastWrite: Thu Oct 1 00:37:14 2015 Z

SN: 07032B5A180AA664&0

Vol Name: THUMBDRIVE

VSN: B650-E7C9

Disk&Ven\_&Prod\_&Rev\_PMAP

LastWrite: Tue Sep 29 20:03:30 2015 Z

SN: 07032B5A180AA664&0

Vol Name: THUMBDRIVE

VSN: F86E-7DF0

## SOFTWARE OUTPUT

## Disk&amp;Ven\_&amp;Prod\_&amp;Rev\_PMAP

LastWrite: Thu Oct 1 23:47:44 2015 Z

SN: 070B43D2DE271C28&amp;0

Vol Name: USB DISK

VSN: FEB5-787A

## Disk&amp;Ven\_&amp;Prod\_&amp;Rev\_PMAP

LastWrite: Sat Mar 19 22:25:27 2016 Z

SN: 070B43D9AB6E9253&amp;0

Vol Name: USB DISK

VSN: 5AE9-6B9E

## Disk&amp;Ven\_&amp;Prod\_&amp;Rev\_PMAP

LastWrite: Sat Mar 19 22:39:41 2016 Z

SN: 070B43D9AB6E9253&amp;0

Vol Name: USB DISK

VSN: 3438-1EDD

## Disk&amp;Ven\_Apple&amp;Prod\_iPod&amp;Rev\_2.70

LastWrite: Thu Nov 19 17:48:02 2015 Z

SN: 000A27001CA9A995&amp;0

Vol Name: ABE MALLIK'

VSN: 32F2-C9BC

## Disk&amp;Ven\_Apple&amp;Prod\_iPod&amp;Rev\_2.70

LastWrite: Thu Nov 19 20:59:35 2015 Z

SN: 000A27001CA9A995&amp;0

Vol Name: ABE-ARJUN M

VSN: DC14-ED4A

## Disk&amp;Ven\_Apple&amp;Prod\_iPod&amp;Rev\_2.70

LastWrite: Thu Nov 19 20:58:49 2015 Z

SN: 000A27001CA9A995&amp;0

Vol Name: IPOD

VSN: DC14-ED4A

## Disk&amp;Ven\_hp&amp;Prod\_USB\_FLASH\_DRIVE&amp;Rev\_1.00

LastWrite: Sat Sep 12 01:43:24 2015 Z

SN: 002354D46B97AC5102CF01C0&amp;0

Vol Name: EEO 2014

VSN: 5267-529A

## Disk&amp;Ven\_hp&amp;Prod\_USB\_FLASH\_DRIVE&amp;Rev\_1.00

LastWrite: Sat Sep 12 02:14:41 2015 Z

SN: 002354D46B97AC5102CF01C0&amp;0

Vol Name: EEO 2014

VSN: 2CC2-CDDB

## SOFTWARE OUTPUT

Disk&Ven\_hp&Prod\_USB\_FLASH\_DRIVE&Rev\_1.00

LastWrite: Sat Sep 12 04:23:52 2015 Z

SN: 002354D46B97AC5102CF01C0&0

Vol Name: ITUNES

VSN: 2CC2-CDDb

LastTestedTime: Sat Sep 12 04:23:52 2015 Z

Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_1100

LastWrite: Thu Oct 8 00:17:58 2015 Z

SN: ACB3HD1000000240&0

Vol Name: EEO 2014

VSN: 7E6C-12B9

Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_1100

LastWrite: Thu Oct 8 00:20:58 2015 Z

SN: ACB3HD1000000240&0

Vol Name: EEO 2014

VSN: 8A30-CC6A

Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_1100

LastWrite: Thu Oct 8 00:20:45 2015 Z

SN: ACB3HD1000000240&0

Vol Name: EEO 2014

VSN: 9E28-AC17

Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_1100

LastWrite: Sat Nov 28 20:16:52 2015 Z

SN: ACB3HD1000000240&0

Vol Name: PHOTOS

VSN: CC84-6474

Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_1100

LastWrite: Thu Oct 8 00:29:36 2015 Z

SN: ACB3HD1000000240&0

Vol Name: WORKFILES

VSN: 8A30-CC6A

LastTestedTime: Thu Oct 8 00:29:36 2015 Z

Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_1100

LastWrite: Fri Nov 20 01:55:29 2015 Z

SN: ACB3HD1000000240&0

Vol Name: WORKFILES

VSN: CC84-6474

Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_8192

LastWrite: Mon Oct 19 13:06:32 2015 Z

SN: AABA1ECC00001167&0



## SOFTWARE OUTPUT

Vol Name: USB20FD

VSN: 3012-1441

Disk&Ven\_SanDisk&Prod\_Cruzer&Rev\_1.20

LastWrite: Mon Oct 26 09:56:40 2015 Z

SN: 200544568018E7B0762E&0

VSN: 2099-41D8

LastTestedTime: Mon Oct 26 09:56:40 2015 Z

Disk&Ven\_SanDisk&Prod\_Cruzer\_Micro&Rev\_8.02

LastWrite: Wed Apr 6 14:25:02 2016 Z

SN: 2243400CB8E0533D&0

VSN: 782F-12D2

Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00

LastWrite: Fri Nov 20 01:55:57 2015 Z

SN: C68B200FB019&0

VSN: 92AC-F638

Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00

LastWrite: Fri Nov 20 01:55:57 2015 Z

SN: C68B200FB019&1

VSN: 0

Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00

LastWrite: Fri Nov 20 01:55:55 2015 Z

SN: C68B200FB019&2

Vol Name: PMHOME

VSN: 0

-----  
ie\_version v.20140717

(Software) Get IE version and build

Microsoft\Internet Explorer

LastWrite Time Wed Apr 13 11:40:56 2016 (UTC)

IE Build = 99600

IE Version = 9.11.9600.18282

svcUpdateVersion (IE 10/11) = 11.0.30

svcVersion (IE 10/11) = 11.0.9600.18282

-----  
imagefile v.20131007

(Software) Checks IFEO subkeys for Debugger & CWDIllegalInDllSearch values

Microsoft\Windows NT\CurrentVersion\Image File Execution Options

No Debugger/CWDIllegalInDllSearch values found.

## SOFTWARE OUTPUT

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options not found.

-----  
init\_dlls v.20110309

(Software) Check for odd \*\*pInit\_Dlls keys

init\_dlls

Microsoft\Windows NT\CurrentVersion\Windows

LastWrite: Tue Jul 14 04:53:25 2009

LoadAppInit\_DLLs

LoadAppInit\_DLLs

-----  
installedcomp v.20130911

(Software) Get info about Installed Components and StubPath values

Microsoft\Active Setup\Installed Components

LastWrite Time Mon Dec 21 11:42:17 2015 (UTC)

Wed Apr 20 15:39:52 2016 (UTC),{3af36230-a269-11d1-b5bf-0000f8051515},MobilePk,  
v.11,0,9600,18163

Wed Apr 20 15:39:52 2016 (UTC),{45ea75a0-a269-11d1-b5bf-0000f8051515},HelpCont,  
v.11,0,9600,18163

Wed Apr 20 15:39:52 2016 (UTC),{5fd399c0-a70a-11d1-9948-00c04f98bbc9},GenSetup,  
v.11,0,9600,18163

Wed Apr 20 15:39:52 2016 (UTC),{630b1da0-b465-11d1-9948-00c04f98bbc9},ExtraPack,  
v.11,0,9600,18163

Wed Apr 20 15:39:52 2016 (UTC),{66C64F22-FC60-4E6C-A6B5-F0D580E680CE},  
v.11,0,9600,0, C:\WINDOWS\System32\ie4uunit.exe -EnableTLS

Wed Apr 20 15:39:52 2016 (UTC),{9381D8F2-0288-11D0-9501-00AA00B911A5},Tridata,  
v.11,0,9600,18163

Wed Apr 20 15:39:52 2016 (UTC),{de5aed00-a4bf-11d1-9948-00c04f98bbc9},HTMLHelp,  
v.6,3,9600,18163

Wed Apr 20 15:39:52 2016 (UTC),{3af36230-a269-11d1-b5bf-0000f8051515},MobilePk,  
v.11,0,9600,18163

Wed Apr 20 15:39:52 2016 (UTC),{45ea75a0-a269-11d1-b5bf-0000f8051515},HelpCont,  
v.11,0,9600,18163

Wed Apr 20 15:39:52 2016 (UTC),{5fd399c0-a70a-11d1-9948-00c04f98bbc9},GenSetup,  
v.11,0,9600,18163

Wed Apr 20 15:39:52 2016 (UTC),{630b1da0-b465-11d1-9948-00c04f98bbc9},ExtraPack,  
v.11,0,9600,18163

Wed Apr 20 15:39:52 2016 (UTC),{9381D8F2-0288-11D0-9501-00AA00B911A5},Tridata,  
v.11,0,9600,18163

Wed Apr 20 15:39:52 2016 (UTC),{de5aed00-a4bf-11d1-9948-00c04f98bbc9},HTMLHelp,  
v.6,3,9600,18163

Tue Apr 19 20:41:00 2016 (UTC),{8A69D345-D564-463c-AFF1-A69D9E530F96}, v.43,0,0,0,  
"C:\Program Files

(x86)\Google\Chrome\Application\50.0.2661.75\Installer\chromstp.exe"

## SOFTWARE OUTPUT

```
--configure-user-settings --verbose-logging --system-level --multi-install --chrome
Mon Apr 18 15:54:27 2016 (UTC),{08B0E5C0-4FCB-11CF-AAA5-00401C608500},JAVAVM,
v.5,0,5000,0
Mon Apr 18 15:51:12 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4383},
Mon Apr 18 15:51:11 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4383},BASEIE40_W2K,
v.11,0,9600,0, C:\WINDOWS\System32\ie4uinit.exe -UserConfig
Mon Apr 18 15:50:45 2016 (UTC),{7D715857-A67C-4C2F-A929-038448584D63},
v.11,0,9600,0, C:\WINDOWS\System32\ie4uinit.exe -DisableSSL3
Mon Apr 18 15:50:45 2016 (UTC),{C9E9A340-D1F1-11D0-821E-444553540600},Fontcore,
v.11,0,9600,0
Mon Apr 18 15:50:45 2016 (UTC),{C9E9A340-D1F1-11D0-821E-444553540600},Fontcore,
v.11,0,9600,0
Wed Apr 13 11:40:56 2016 (UTC),{3af36230-a269-11d1-b5bf-0000f8051515},MobilePk,
v.11,0,9600,18282
Wed Apr 13 11:40:56 2016 (UTC),{45ea75a0-a269-11d1-b5bf-0000f8051515},HelpCont,
v.11,0,9600,18282
Wed Apr 13 11:40:56 2016 (UTC),{5fd399c0-a70a-11d1-9948-00c04f98bbc9},GenSetup,
v.11,0,9600,18282
Wed Apr 13 11:40:56 2016 (UTC),{630b1da0-b465-11d1-9948-00c04f98bbc9},ExtraPack,
v.11,0,9600,18282
Wed Apr 13 11:40:56 2016 (UTC),{9381D8F2-0288-11D0-9501-00AA00B911A5},Tridata,
v.11,0,9600,18282
Wed Apr 13 11:40:56 2016 (UTC),{de5aed00-a4bf-11d1-9948-00c04f98bbc9},HTMLHelp,
v.6,3,9600,18282
Thu Mar 10 13:50:00 2016 (UTC),>{22d6f312-b0f6-11d0-94ab-0080c74c7e95},WMPACCESS,
v.12,0,7601,19148, %SystemRoot%\system32\unregmp2.exe /ShowWMP
Thu Mar 10 13:50:00 2016 (UTC),{22d6f312-b0f6-11d0-94ab-0080c74c7e95},
v.12,0,7601,19148
Thu Mar 10 13:50:00 2016 (UTC),{6BF52A52-394A-11d3-B153-00C04F79FAA6},Microsoft
Windows Media Player, v.12,0,7601,19148, %SystemRoot%\system32\unregmp2.exe
/FirstLogon /Shortcuts /RegBrowsers /ResetMUI
Wed Feb 10 01:11:16 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4340},IE4_SHELLID,
v.6,1,7601,23338, regsvr32.exe /s /n /i:U shell32.dll
Wed Dec 30 12:50:33 2015
(UTC),{2D46B6DC-2207-486B-B523-A557E6D54B47},ClearIconCache, v.11,0,9600,16428,
C:\windows\system32\cmd.exe /D /C start C:\windows\system32\ie4uinit.exe
-ClearIconCache
Wed Dec 30 12:48:40 2015 (UTC),{6fab99d0-bab8-11d1-994a-00c04f98bbc9},MSN_Auth,
v.4,9,9,2
Wed Dec 30 07:41:07 2015 (UTC),>{22d6f312-b0f6-11d0-94ab-0080c74c7e95},WMPACCESS,
v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe /ShowWMP
Wed Dec 30 07:41:07 2015 (UTC),{22d6f312-b0f6-11d0-94ab-0080c74c7e95},
v.12,0,7601,18840
Wed Dec 30 07:41:07 2015 (UTC),{6BF52A52-394A-11d3-B153-00C04F79FAA6},Microsoft
Windows Media Player, v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe
/FirstLogon /Shortcuts /RegBrowsers /ResetMUI
Wed Dec 30 07:41:07 2015 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4340},IE4_SHELLID,
v.6,1,7601,18952, regsvr32.exe /s /n /i:U shell32.dll
```

## SOFTWARE OUTPUT

Wed Dec 30 07:41:07 2015 (UTC),>{22d6f312-b0f6-11d0-94ab-0080c74c7e95},WMPACCESS,  
v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe /ShowWMP

Wed Dec 30 07:41:07 2015 (UTC),{22d6f312-b0f6-11d0-94ab-0080c74c7e95},  
v.12,0,7601,18840

Wed Dec 30 07:41:07 2015 (UTC),{6BF52A52-394A-11d3-B153-00C04F79FAA6},Microsoft  
Windows Media Player, v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe  
/FirstLogon /Shortcuts /RegBrowsers /ResetMUI

Wed Dec 30 07:41:07 2015 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4340},IE4\_SHELLID,  
v.6,1,7601,18952, regsvr32.exe /s /n /i:U shell32.dll

Wed Dec 30 07:06:36 2015 (UTC),{0EEB34F6-991D-4a1b-8EEB-772DA0EADB22},Microsoft Lync  
2010, v.4.0.7577.4486

Tue Dec 29 18:43:08 2015  
(UTC),{89B4C1CD-B018-4511-B0A1-5476DBF70820},DOTNETFRAMEWORKS,,  
C:\Windows\system32\Rundll32.exe C:\Windows\system32\mscories.dll,Install

Tue Dec 29 18:43:08 2015  
(UTC),{89B4C1CD-B018-4511-B0A1-5476DBF70820},DOTNETFRAMEWORKS,,  
C:\Windows\SysWOW64\Rundll32.exe C:\Windows\SysWOW64\mscories.dll,Install

Tue Dec 29 18:23:34 2015 (UTC),{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4},.NETFramework,  
v.4,0,30319,0

Tue Dec 29 18:23:33 2015 (UTC),{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4},.NETFramework,  
v.4,0,30319,0

Mon Dec 21 11:42:17 2015 (UTC),{26784146-6E05-3FF9-9335-786C7C0FB5BE},.NETFramework,  
v.4,0,30319,0

Tue Oct 20 00:49:16 2015 (UTC),{66C64F22-FC60-4E6C-A6B5-F0D580E680CE},  
v.11,0,9600,0, C:\Windows\System32\ie4uinit.exe -EnableTLS

Sat Sep 12 00:14:20 2015 (UTC),{1AD147D0-BE0E-3D6C-AC11-64F6DC4163F1},.NETFramework,  
v.4,0,30319,0

Thu Sep 10 21:48:07 2015 (UTC),{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4},.NETFramework,  
v.4,0,30319,0

Thu Sep 10 20:46:43 2015 (UTC),{7D715857-A67C-4C2F-A929-038448584D63},  
v.11,0,9600,0, C:\Windows\System32\ie4uinit.exe -DisableSSL3

Mon Dec 1 14:13:55 2014 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4383},BASEIE40\_W2K,  
v.11,0,9600,0, C:\Windows\System32\ie4uinit.exe -UserConfig

Mon Dec 1 14:13:22 2014 (UTC),{C9E9A340-D1F1-11D0-821E-444553540600},Fontcore,  
v.11,0,9600,0

Sun Nov 21 03:33:56 2010 (UTC),{44BBA840-CC51-11CF-AAFA-00AA00B6015C},MailNews,  
v.6,1,7601,17514, "%ProgramFiles%\Windows Mail\WinMail.exe" OCInstallUserConfigOE

Sun Nov 21 03:33:56 2010 (UTC),{7790769C-0471-11d2-AF11-00C04FA35D02},  
v.6,1,7601,17514

Sun Nov 21 03:33:56 2010 (UTC),{44BBA840-CC51-11CF-AAFA-00AA00B6015C},MailNews,  
v.6,1,7601,17514, "%ProgramFiles(x86)%\Windows Mail\WinMail.exe"  
OCInstallUserConfigOE

Sun Nov 21 03:33:56 2010 (UTC),{7790769C-0471-11d2-AF11-00C04FA35D02},  
v.6,1,7601,17514

Sun Nov 21 03:33:56 2010 (UTC),{44BBA840-CC51-11CF-AAFA-00AA00B6015C},MailNews,  
v.6,1,7601,17514, "%ProgramFiles%\Windows Mail\WinMail.exe" OCInstallUserConfigOE

Sun Nov 21 03:33:56 2010 (UTC),{7790769C-0471-11d2-AF11-00C04FA35D02},  
v.6,1,7601,17514

## SOFTWARE OUTPUT

Tue Jul 14 04:49:55 2009 (UTC),{FEBEF00C-046D-438D-8A88-BF94A6C9E703},.NETFramework,  
 v.2,0,50727,0  
 Tue Jul 14 04:49:55 2009 (UTC),{7C028AF8-F614-47B3-82DA-BA94E41B1089},.NETFramework,  
 v.2,0,50727,0  
 Tue Jul 14 04:49:55 2009 (UTC),{FEBEF00C-046D-438D-8A88-BF94A6C9E703},.NETFramework,  
 v.2,0,50727,0  
 Tue Jul 14 04:49:04 2009 (UTC),{2C7339CF-2B09-4501-B3F3-F3508C9228ED},Theme  
 Component, v.1,1,1,9, %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall  
 %SystemRoot%\system32\themeui.dll  
 Tue Jul 14 04:49:04 2009 (UTC),{44BBA855-CC51-11CF-AAFA-00AA00B6015F},DirectDrawEx,  
 v.4,71,1113,0  
 Tue Jul 14 04:49:04 2009 (UTC),{4f645220-306d-11d2-995d-00c04f98bbc9},MSVBScript,  
 v.5,6,0,8833  
 Tue Jul 14 04:49:04 2009 (UTC),{E92B03AB-B707-11d2-9CBD-0000F87A369E},ADSI,  
 v.5,0,00,0  
 Tue Jul 14 04:49:00 2009 (UTC),{2C7339CF-2B09-4501-B3F3-F3508C9228ED},Theme  
 Component, v.1,1,1,9, %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall  
 %SystemRoot%\system32\themeui.dll  
 Tue Jul 14 04:49:00 2009 (UTC),{44BBA855-CC51-11CF-AAFA-00AA00B6015F},DirectDrawEx,  
 v.4,71,1113,0  
 Tue Jul 14 04:49:00 2009 (UTC),{4f645220-306d-11d2-995d-00c04f98bbc9},MSVBScript,  
 v.5,6,0,8833  
 Tue Jul 14 04:49:00 2009 (UTC),{6fab99d0-bab8-11d1-994a-00c04f98bbc9},MSN\_Auth,  
 v.4,9,9,2  
 Tue Jul 14 04:49:00 2009 (UTC),{E92B03AB-B707-11d2-9CBD-0000F87A369E},ADSI,  
 v.5,0,00,0  
 Tue Jul 14 04:49:00 2009 (UTC),{2C7339CF-2B09-4501-B3F3-F3508C9228ED},Theme  
 Component, v.1,1,1,9, %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall  
 %SystemRoot%\system32\themeui.dll  
 Tue Jul 14 04:49:00 2009 (UTC),{44BBA855-CC51-11CF-AAFA-00AA00B6015F},DirectDrawEx,  
 v.4,71,1113,0  
 Tue Jul 14 04:49:00 2009 (UTC),{4f645220-306d-11d2-995d-00c04f98bbc9},MSVBScript,  
 v.5,6,0,8833  
 Tue Jul 14 04:49:00 2009 (UTC),{6fab99d0-bab8-11d1-994a-00c04f98bbc9},MSN\_Auth,  
 v.4,9,9,2  
 Tue Jul 14 04:49:00 2009 (UTC),{E92B03AB-B707-11d2-9CBD-0000F87A369E},ADSI,  
 v.5,0,00,0

Wow6432Node\Microsoft\Active Setup\Installed Components  
 LastWrite Time Mon Dec 21 11:42:16 2015 (UTC)

Wed Apr 20 15:39:52 2016 (UTC),{3af36230-a269-11d1-b5bf-0000f8051515},MobilePk,  
 v.11,0,9600,18163  
 Wed Apr 20 15:39:52 2016 (UTC),{45ea75a0-a269-11d1-b5bf-0000f8051515},HelpCont,  
 v.11,0,9600,18163  
 Wed Apr 20 15:39:52 2016 (UTC),{5fd399c0-a70a-11d1-9948-00c04f98bbc9},GenSetup,  
 v.11,0,9600,18163  
 Wed Apr 20 15:39:52 2016 (UTC),{630b1da0-b465-11d1-9948-00c04f98bbc9},ExtraPack,

## SOFTWARE OUTPUT

```

v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{66C64F22-FC60-4E6C-A6B5-F0D580E680CE},
v.11,0,9600,0, C:\WINDOWS\System32\ie4uinit.exe -EnableTLS
Wed Apr 20 15:39:52 2016 (UTC),{9381D8F2-0288-11D0-9501-00AA00B911A5},Tridata,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{de5aed00-a4bf-11d1-9948-00c04f98bbc9},HTMLHelp,
v.6,3,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{3af36230-a269-11d1-b5bf-0000f8051515},MobilePk,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{45ea75a0-a269-11d1-b5bf-0000f8051515},HelpCont,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{5fd399c0-a70a-11d1-9948-00c04f98bbc9},GenSetup,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{630b1da0-b465-11d1-9948-00c04f98bbc9},ExtraPack,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{9381D8F2-0288-11D0-9501-00AA00B911A5},Tridata,
v.11,0,9600,18163
Wed Apr 20 15:39:52 2016 (UTC),{de5aed00-a4bf-11d1-9948-00c04f98bbc9},HTMLHelp,
v.6,3,9600,18163
Tue Apr 19 20:41:00 2016 (UTC),{8A69D345-D564-463c-AFF1-A69D9E530F96}, v.43,0,0,0,
"C:\Program Files
(x86)\Google\Chrome\Application\50.0.2661.75\Installer\chromstp.exe"
--configure-user-settings --verbose-logging --system-level --multi-install --chrome
Mon Apr 18 15:54:27 2016 (UTC),{08B0E5C0-4FCB-11CF-AAA5-00401C608500},JAVAVM,
v.5,0,5000,0
Mon Apr 18 15:51:12 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4383},
Mon Apr 18 15:51:11 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4383},BASEIE40_W2K,
v.11,0,9600,0, C:\WINDOWS\System32\ie4uinit.exe -UserConfig
Mon Apr 18 15:50:45 2016 (UTC),{7D715857-A67C-4C2F-A929-038448584D63},
v.11,0,9600,0, C:\WINDOWS\System32\ie4uinit.exe -DisableSSL3
Mon Apr 18 15:50:45 2016 (UTC),{C9E9A340-D1F1-11D0-821E-444553540600},Fontcore,
v.11,0,9600,0
Mon Apr 18 15:50:45 2016 (UTC),{C9E9A340-D1F1-11D0-821E-444553540600},Fontcore,
v.11,0,9600,0
Wed Apr 13 11:40:56 2016 (UTC),{3af36230-a269-11d1-b5bf-0000f8051515},MobilePk,
v.11,0,9600,18282
Wed Apr 13 11:40:56 2016 (UTC),{45ea75a0-a269-11d1-b5bf-0000f8051515},HelpCont,
v.11,0,9600,18282
Wed Apr 13 11:40:56 2016 (UTC),{5fd399c0-a70a-11d1-9948-00c04f98bbc9},GenSetup,
v.11,0,9600,18282
Wed Apr 13 11:40:56 2016 (UTC),{630b1da0-b465-11d1-9948-00c04f98bbc9},ExtraPack,
v.11,0,9600,18282
Wed Apr 13 11:40:56 2016 (UTC),{9381D8F2-0288-11D0-9501-00AA00B911A5},Tridata,
v.11,0,9600,18282
Wed Apr 13 11:40:56 2016 (UTC),{de5aed00-a4bf-11d1-9948-00c04f98bbc9},HTMLHelp,
v.6,3,9600,18282
Wed Apr 13 11:40:56 2016 (UTC),{3af36230-a269-11d1-b5bf-0000f8051515},MobilePk,
v.11,0,9600,18282

```

## SOFTWARE OUTPUT

Wed Apr 13 11:40:56 2016 (UTC),{45ea75a0-a269-11d1-b5bf-0000f8051515},HelpCont,  
v.11,0,9600,18282

Wed Apr 13 11:40:56 2016 (UTC),{5fd399c0-a70a-11d1-9948-00c04f98bbc9},GenSetup,  
v.11,0,9600,18282

Wed Apr 13 11:40:56 2016 (UTC),{630b1da0-b465-11d1-9948-00c04f98bbc9},ExtraPack,  
v.11,0,9600,18282

Wed Apr 13 11:40:56 2016 (UTC),{9381D8F2-0288-11D0-9501-00AA00B911A5},Tridata,  
v.11,0,9600,18282

Wed Apr 13 11:40:56 2016 (UTC),{de5aed00-a4bf-11d1-9948-00c04f98bbc9},HTMLHelp,  
v.6,3,9600,18282

Thu Mar 10 13:50:00 2016 (UTC),>{22d6f312-b0f6-11d0-94ab-0080c74c7e95},WMPACCESS,  
v.12,0,7601,19148, %SystemRoot%\system32\unregmp2.exe /ShowWMP

Thu Mar 10 13:50:00 2016 (UTC),{22d6f312-b0f6-11d0-94ab-0080c74c7e95},  
v.12,0,7601,19148

Thu Mar 10 13:50:00 2016 (UTC),{6BF52A52-394A-11d3-B153-00C04F79FAA6},Microsoft  
Windows Media Player, v.12,0,7601,19148, %SystemRoot%\system32\unregmp2.exe  
/FirstLogon /Shortcuts /RegBrowsers /ResetMUI

Thu Mar 10 13:50:00 2016 (UTC),>{22d6f312-b0f6-11d0-94ab-0080c74c7e95},WMPACCESS,  
v.12,0,7601,19148, %SystemRoot%\system32\unregmp2.exe /ShowWMP

Thu Mar 10 13:50:00 2016 (UTC),{22d6f312-b0f6-11d0-94ab-0080c74c7e95},  
v.12,0,7601,19148

Thu Mar 10 13:50:00 2016 (UTC),{6BF52A52-394A-11d3-B153-00C04F79FAA6},Microsoft  
Windows Media Player, v.12,0,7601,19148, %SystemRoot%\system32\unregmp2.exe  
/FirstLogon /Shortcuts /RegBrowsers /ResetMUI

Fri Feb 19 22:20:57 2016 (UTC),{8A69D345-D564-463c-AFF1-A69D9E530F96}, v.43,0,0,0,  
"C:\Program Files  
(x86)\Google\Chrome\Application\48.0.2564.116\Installer\chrmstp.exe"  
--configure-user-settings --verbose-logging --system-level --multi-install --chrome

Wed Feb 10 01:11:16 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4340},IE4\_SHELLID,  
v.6,1,7601,23338, regsvr32.exe /s /n /i:U shell32.dll

Wed Feb 10 01:11:16 2016 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4340},IE4\_SHELLID,  
v.6,1,7601,23338, regsvr32.exe /s /n /i:U shell32.dll

Wed Dec 30 12:50:33 2015  
(UTC),{2D46B6DC-2207-486B-B523-A557E6D54B47},ClearIconCache, v.11,0,9600,16428,  
C:\windows\system32\cmd.exe /D /C start C:\windows\system32\ie4uinit.exe  
-ClearIconCache

Wed Dec 30 12:48:40 2015 (UTC),{6fab99d0-bab8-11d1-994a-00c04f98bbc9},MSN\_Auth,  
v.4,9,9,2

Wed Dec 30 07:41:07 2015 (UTC),>{22d6f312-b0f6-11d0-94ab-0080c74c7e95},WMPACCESS,  
v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe /ShowWMP

Wed Dec 30 07:41:07 2015 (UTC),{22d6f312-b0f6-11d0-94ab-0080c74c7e95},  
v.12,0,7601,18840

Wed Dec 30 07:41:07 2015 (UTC),{6BF52A52-394A-11d3-B153-00C04F79FAA6},Microsoft  
Windows Media Player, v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe  
/FirstLogon /Shortcuts /RegBrowsers /ResetMUI

Wed Dec 30 07:41:07 2015 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4340},IE4\_SHELLID,  
v.6,1,7601,18952, regsvr32.exe /s /n /i:U shell32.dll

Wed Dec 30 07:41:07 2015 (UTC),>{22d6f312-b0f6-11d0-94ab-0080c74c7e95},WMPACCESS,

## SOFTWARE OUTPUT

v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe /ShowWMP  
 Wed Dec 30 07:41:07 2015 (UTC),{22d6f312-b0f6-11d0-94ab-0080c74c7e95},  
 v.12,0,7601,18840  
 Wed Dec 30 07:41:07 2015 (UTC),{6BF52A52-394A-11d3-B153-00C04F79FAA6},Microsoft  
 Windows Media Player, v.12,0,7601,18840, %SystemRoot%\system32\unregmp2.exe  
 /FirstLogon /Shortcuts /RegBrowsers /ResetMUI  
 Wed Dec 30 07:41:07 2015 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4340},IE4\_SHELLID,  
 v.6,1,7601,18952, regsvr32.exe /s /n /i:U shell32.dll  
 Wed Dec 30 07:06:36 2015 (UTC),{0EEB34F6-991D-4a1b-8EEB-772DA0EADB22},Microsoft Lync  
 2010, v.4.0.7577.4486  
 Tue Dec 29 18:43:08 2015  
 (UTC),{89B4C1CD-B018-4511-B0A1-5476DBF70820},DOTNETFRAMEWORKS,,  
 C:\Windows\system32\Rundll32.exe C:\Windows\system32\mscories.dll,Install  
 Tue Dec 29 18:43:08 2015  
 (UTC),{89B4C1CD-B018-4511-B0A1-5476DBF70820},DOTNETFRAMEWORKS,,  
 C:\Windows\SysWOW64\Rundll32.exe C:\Windows\SysWOW64\mscories.dll,Install  
 Tue Dec 29 18:23:34 2015 (UTC),{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4},.NETFramework,  
 v.4,0,30319,0  
 Tue Dec 29 18:23:33 2015 (UTC),{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4},.NETFramework,  
 v.4,0,30319,0  
 Mon Dec 21 11:42:17 2015 (UTC),{26784146-6E05-3FF9-9335-786C7C0FB5BE},.NETFramework,  
 v.4,0,30319,0  
 Mon Dec 21 11:42:16 2015 (UTC),{26784146-6E05-3FF9-9335-786C7C0FB5BE},.NETFramework,  
 v.4,0,30319,0  
 Tue Oct 20 00:49:16 2015 (UTC),{66C64F22-FC60-4E6C-A6B5-F0D580E680CE},  
 v.11,0,9600,0, C:\Windows\System32\ie4uinit.exe -EnableTLS  
 Sat Sep 12 00:14:20 2015 (UTC),{1AD147D0-BE0E-3D6C-AC11-64F6DC4163F1},.NETFramework,  
 v.4,0,30319,0  
 Sat Sep 12 00:14:19 2015 (UTC),{1AD147D0-BE0E-3D6C-AC11-64F6DC4163F1},.NETFramework,  
 v.4,0,30319,0  
 Thu Sep 10 21:48:07 2015 (UTC),{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4},.NETFramework,  
 v.4,0,30319,0  
 Thu Sep 10 21:48:06 2015 (UTC),{F5B09CFD-F0B2-36AF-8DF4-1DF6B63FC7B4},.NETFramework,  
 v.4,0,30319,0  
 Thu Sep 10 20:46:43 2015 (UTC),{7D715857-A67C-4C2F-A929-038448584D63},  
 v.11,0,9600,0, C:\Windows\System32\ie4uinit.exe -DisableSSL3  
 Mon Dec 1 14:13:55 2014 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4383},BASEIE40\_W2K,  
 v.11,0,9600,0, C:\Windows\System32\ie4uinit.exe -UserConfig  
 Mon Dec 1 14:13:55 2014 (UTC),{89820200-ECBD-11cf-8B85-00AA005B4383},  
 Mon Dec 1 14:13:22 2014 (UTC),{C9E9A340-D1F1-11D0-821E-444553540600},Fontcore,  
 v.11,0,9600,0  
 Mon Dec 1 14:13:22 2014 (UTC),{C9E9A340-D1F1-11D0-821E-444553540600},Fontcore,  
 v.11,0,9600,0  
 Mon Dec 1 12:56:43 2014  
 (UTC),{89B4C1CD-B018-4511-B0A1-5476DBF70820},DOTNETFRAMEWORKS,,  
 C:\Windows\SysWOW64\Rundll32.exe C:\Windows\SysWOW64\mscories.dll,Install  
 Sun Nov 21 03:33:56 2010 (UTC),{44BBA840-CC51-11CF-AAFA-00AA00B6015C},MailNews,  
 v.6,1,7601,17514, "%ProgramFiles%\Windows Mail\WinMail.exe" OCInstallUserConfigOE



## SOFTWARE OUTPUT

Sun Nov 21 03:33:56 2010 (UTC),{7790769C-0471-11d2-AF11-00C04FA35D02},  
v.6,1,7601,17514  
Sun Nov 21 03:33:56 2010 (UTC),{44BBA840-CC51-11CF-AAFA-00AA00B6015C},MailNews,  
v.6,1,7601,17514, "%ProgramFiles(x86)%\Windows Mail\WinMail.exe"  
OCInstallUserConfigOE  
Sun Nov 21 03:33:56 2010 (UTC),{7790769C-0471-11d2-AF11-00C04FA35D02},  
v.6,1,7601,17514  
Sun Nov 21 03:33:56 2010 (UTC),{44BBA840-CC51-11CF-AAFA-00AA00B6015C},MailNews,  
v.6,1,7601,17514, "%ProgramFiles%\Windows Mail\WinMail.exe" OCInstallUserConfigOE  
Sun Nov 21 03:33:56 2010 (UTC),{7790769C-0471-11d2-AF11-00C04FA35D02},  
v.6,1,7601,17514  
Sun Nov 21 03:33:56 2010 (UTC),{44BBA840-CC51-11CF-AAFA-00AA00B6015C},MailNews,  
v.6,1,7601,17514, "%ProgramFiles(x86)%\Windows Mail\WinMail.exe"  
OCInstallUserConfigOE  
Sun Nov 21 03:33:56 2010 (UTC),{7790769C-0471-11d2-AF11-00C04FA35D02},  
v.6,1,7601,17514  
Tue Jul 14 04:49:55 2009 (UTC),{FEBEF00C-046D-438D-8A88-BF94A6C9E703},.NETFramework,  
v.2,0,50727,0  
Tue Jul 14 04:49:55 2009 (UTC),{7C028AF8-F614-47B3-82DA-BA94E41B1089},.NETFramework,  
v.2,0,50727,0  
Tue Jul 14 04:49:55 2009 (UTC),{FEBEF00C-046D-438D-8A88-BF94A6C9E703},.NETFramework,  
v.2,0,50727,0  
Tue Jul 14 04:49:55 2009 (UTC),{7C028AF8-F614-47B3-82DA-BA94E41B1089},.NETFramework,  
v.2,0,50727,0  
Tue Jul 14 04:49:04 2009 (UTC),{2C7339CF-2B09-4501-B3F3-F3508C9228ED},Theme  
Component, v.1,1,1,9, %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall  
%SystemRoot%\system32\themeui.dll  
Tue Jul 14 04:49:04 2009 (UTC),{44BBA855-CC51-11CF-AAFA-00AA00B6015F},DirectDrawEx,  
v.4,71,1113,0  
Tue Jul 14 04:49:04 2009 (UTC),{4f645220-306d-11d2-995d-00c04f98bbc9},MSVBScript,  
v.5,6,0,8833  
Tue Jul 14 04:49:04 2009 (UTC),{E92B03AB-B707-11d2-9CBD-0000F87A369E},ADSI,  
v.5,0,00,0  
Tue Jul 14 04:49:04 2009 (UTC),{2C7339CF-2B09-4501-B3F3-F3508C9228ED},Theme  
Component, v.1,1,1,9, %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall  
%SystemRoot%\system32\themeui.dll  
Tue Jul 14 04:49:04 2009 (UTC),{44BBA855-CC51-11CF-AAFA-00AA00B6015F},DirectDrawEx,  
v.4,71,1113,0  
Tue Jul 14 04:49:04 2009 (UTC),{4f645220-306d-11d2-995d-00c04f98bbc9},MSVBScript,  
v.5,6,0,8833  
Tue Jul 14 04:49:04 2009 (UTC),{6fab99d0-bab8-11d1-994a-00c04f98bbc9},MSN\_Auth,  
v.4,9,9,2  
Tue Jul 14 04:49:04 2009 (UTC),{E92B03AB-B707-11d2-9CBD-0000F87A369E},ADSI,  
v.5,0,00,0  
Tue Jul 14 04:49:00 2009 (UTC),{2C7339CF-2B09-4501-B3F3-F3508C9228ED},Theme  
Component, v.1,1,1,9, %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall  
%SystemRoot%\system32\themeui.dll  
Tue Jul 14 04:49:00 2009 (UTC),{44BBA855-CC51-11CF-AAFA-00AA00B6015F},DirectDrawEx,

## SOFTWARE OUTPUT

```

v.4,71,1113,0
Tue Jul 14 04:49:00 2009 (UTC),{4f645220-306d-11d2-995d-00c04f98bbc9},MSVBScript,
v.5,6,0,8833
Tue Jul 14 04:49:00 2009 (UTC),{6fab99d0-bab8-11d1-994a-00c04f98bbc9},MSN_Auth,
v.4,9,9,2
Tue Jul 14 04:49:00 2009 (UTC),{E92B03AB-B707-11d2-9CBD-0000F87A369E},ADSI,
v.5,0,00,0
Tue Jul 14 04:49:00 2009 (UTC),{2C7339CF-2B09-4501-B3F3-F3508C9228ED},Theme
Component, v.1,1,1,9, %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall
%SystemRoot%\system32\themeui.dll
Tue Jul 14 04:49:00 2009 (UTC),{44BBA855-CC51-11CF-AAFA-00AA00B6015F},DirectDrawEx,
v.4,71,1113,0
Tue Jul 14 04:49:00 2009 (UTC),{4f645220-306d-11d2-995d-00c04f98bbc9},MSVBScript,
v.5,6,0,8833
Tue Jul 14 04:49:00 2009 (UTC),{6fab99d0-bab8-11d1-994a-00c04f98bbc9},MSN_Auth,
v.4,9,9,2
Tue Jul 14 04:49:00 2009 (UTC),{E92B03AB-B707-11d2-9CBD-0000F87A369E},ADSI,
v.5,0,00,0

```

-----  
 Launching installer v.20120917

(Software) Determines product install information

#### Installer

Microsoft\Windows\CurrentVersion\Installer\UserData

User SID: S-1-5-18

Key : 000021091A0090400000000000F01FEC

LastWrite: Thu Sep 10 16:30:42 2015

20150910 - Microsoft Office OneNote MUI (English) 2007 12.0.6612.1000 (Microsoft Corporation)

Key : 00002109511090400000000000F01FEC

LastWrite: Thu Sep 10 16:30:32 2015

20150910 - Microsoft Office Shared Setup Metadata MUI (English) 2007 12.0.6612.1000 (Microsoft Corporation)

Key : 00002109610090400000000000F01FEC

LastWrite: Thu Sep 10 16:30:36 2015

20150910 - Microsoft Office Excel MUI (English) 2007 12.0.6612.1000 (Microsoft Corporation)

Key : 00002109611090400100000000F01FEC

LastWrite: Thu Sep 10 16:30:55 2015

20150910 - Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2007 12.0.6612.1000 (Microsoft Corporation)

Key : 00002109810090400000000000F01FEC

LastWrite: Thu Sep 10 16:30:46 2015

## SOFTWARE OUTPUT

20150910 - Microsoft Office PowerPoint MUI (English) 2007 12.0.6612.1000 (Microsoft Corporation)

Key : 00002109A200000000100000000F01FEC

LastWrite: Thu Sep 10 16:32:34 2015

20150910 - Microsoft Office Office 64-bit Components 2007 12.0.6612.1000 (Microsoft Corporation)

Key : 00002109A200904001000000000F01FEC

LastWrite: Thu Sep 10 16:30:51 2015

20150910 - Microsoft Office Shared 64-bit MUI (English) 2007 12.0.6612.1000 (Microsoft Corporation)

Key : 00002109B100904000000000000F01FEC

LastWrite: Thu Sep 10 16:31:39 2015

20150910 - Microsoft Office Word MUI (English) 2007 12.0.6612.1000 (Microsoft Corporation)

Key : 00002109C200904000000000000F01FEC

LastWrite: Thu Sep 10 16:31:32 2015

20150910 - Microsoft Office Proofing (English) 2007 12.0.4518.1014 (Microsoft Corporation)

Key : 00002109E600904000000000000F01FEC

LastWrite: Thu Sep 10 16:30:23 2015

20151111 - Microsoft Office Shared MUI (English) 2007 12.0.6612.1000 (Microsoft Corporation)

Key : 00002109F100904000000000000F01FEC

LastWrite: Thu Sep 10 16:31:25 2015

20150910 - Microsoft Office Proof (English) 2007 12.0.6612.1000 (Microsoft Corporation)

Key : 00002109F100A0C000000000000F01FEC

LastWrite: Thu Sep 10 16:31:07 2015

20150910 - Microsoft Office Proof (Spanish) 2007 12.0.6612.1000 (Microsoft Corporation)

Key : 00002109F100C04000000000000F01FEC

LastWrite: Thu Sep 10 16:31:15 2015

20150910 - Microsoft Office Proof (French) 2007 12.0.6612.1000 (Microsoft Corporation)

Key : 00002119F200000000000000000F01FEC

LastWrite: Thu Sep 10 16:33:33 2015

20160413 - Microsoft Office Home and Student 2007 12.0.6612.1000 (Microsoft Corporation)

## SOFTWARE OUTPUT

Key : 00004109500200000000000000F01FEC

LastWrite: Thu Sep 10 21:05:18 2015

20150910 - Microsoft Office File Validation Add-In 14.0.5130.5003 (Microsoft Corporation)

Key : 00004109511090400000000000F01FEC

LastWrite: Thu Sep 10 21:27:39 2015

20150910 - Microsoft Office Shared Setup Metadata MUI (English) 2010 14.0.7015.1000 (Microsoft Corporation)

Key : 00004109611090400100000000F01FEC

LastWrite: Thu Sep 10 21:28:02 2015

20150910 - Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2010 14.0.7015.1000 (Microsoft Corporation)

Key : 00004109A100000000000000F01FEC

LastWrite: Thu Sep 10 21:30:17 2015

20160413 - Microsoft Office Outlook 2010 14.0.7015.1000 (Microsoft Corporation)

Key : 00004109A100904000000000F01FEC

LastWrite: Thu Sep 10 21:27:49 2015

20160209 - Microsoft Office Outlook MUI (English) 2010 14.0.7015.1000 (Microsoft Corporation)

Key : 00004109A200000001000000F01FEC

LastWrite: Thu Sep 10 21:28:40 2015

20160310 - Microsoft Office Office 64-bit Components 2010 14.0.7015.1000 (Microsoft Corporation)

Key : 00004109A200904001000000F01FEC

LastWrite: Thu Sep 10 21:27:56 2015

20150910 - Microsoft Office Shared 64-bit MUI (English) 2010 14.0.7015.1000 (Microsoft Corporation)

Key : 00004109C200904000000000F01FEC

LastWrite: Thu Sep 10 21:28:23 2015

20150910 - Microsoft Office Proofing (English) 2010 14.0.7015.1000 (Microsoft Corporation)

Key : 00004109E600904000000000F01FEC

LastWrite: Thu Sep 10 21:27:31 2015

20151111 - Microsoft Office Shared MUI (English) 2010 14.0.7015.1000 (Microsoft Corporation)

Key : 00004109F100904000000000F01FEC

LastWrite: Thu Sep 10 21:28:21 2015

20150910 - Microsoft Office Proof (English) 2010 14.0.7015.1000 (Microsoft Corporation)

## SOFTWARE OUTPUT

Key : 00004109F100A0C00000000000F01FEC  
 LastWrite: Thu Sep 10 21:28:10 2015  
 20150910 - Microsoft Office Proof (Spanish) 2010 14.0.7015.1000 (Microsoft Corporation)

Key : 00004109F100C0400000000000F01FEC  
 LastWrite: Thu Sep 10 21:28:18 2015  
 20150910 - Microsoft Office Proof (French) 2010 14.0.7015.1000 (Microsoft Corporation)

Key : 00004159180090400000000000F01FEC  
 LastWrite: Thu Sep 10 23:33:01 2015  
 20150910 - Microsoft Office Outlook Connector 14.0.6123.5001 (Microsoft Corporation)

Key : 068656828274C334A84D1D9A0334B78C  
 LastWrite: Tue Feb 2 00:21:29 2016  
 20160201 - Nuance PDF Viewer Plus 5.30.3290 (Nuance Communications, Inc)

Key : 09AB59D18F4FCE748A2844C1993DC0E1  
 LastWrite: Thu Feb 4 20:01:57 2016  
 20160204 - MSXML 4.0 SP3 Parser (KB2758694) 4.30.2117.0 (Microsoft Corporation)

Key : 1637AADA8B458CF408E449CEC611DE86  
 LastWrite: Fri Feb 20 17:05:34 2015  
 20150220 - Validity Fingerprint Sensor Driver 4.5.133.0 (Validity Sensors, Inc.)

Key : 1926E8D15D0BCE53481466615F760A7F  
 LastWrite: Thu Sep 10 21:40:31 2015  
 20150910 - Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219 10.0.40219 (Microsoft Corporation)

Key : 1af2a8da7e60d0b429d7e6453b3d0182  
 LastWrite: Thu Feb 4 20:02:22 2016  
 20160204 - Microsoft Visual C++ 2005 Redistributable (x64) 8.0.61000 (Microsoft Corporation)

Key : 1D5E3C0FEDA1E123187686FED06E995A  
 LastWrite: Thu Sep 10 21:40:26 2015  
 20150910 - Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 10.0.40219 (Microsoft Corporation)

Key : 1F764691F11C67F458B88521DA8CB349  
 LastWrite: Tue Feb 2 00:09:45 2016  
 20160201 - MSXML 4.0 SP3 Parser 4.30.2100.0 (Microsoft Corporation)

Key : 1F7F1DFF9CA14CB49A8060686D53BAFA

## SOFTWARE OUTPUT

LastWrite: Thu Jan 7 22:10:30 2016

20160107 - Apple Software Update 2.1.4.131 (Apple Inc.)

Key : 3e43b73803c7c394f8a6b2f0402e19c2

LastWrite: Tue Feb 2 00:11:50 2016

20160201 - Microsoft Visual C++ 2005 Redistributable 8.0.59193 (Microsoft Corporation)

Key : 468C0D80B1125904C8E3D2C2BA46DC9A

LastWrite: Tue Jan 19 22:19:27 2016

20160206 - TurboTax 2015 WinPerFedFormset 015.000.1781 (Intuit Inc.)

Key : 4BEA594979BAED93C82408E6FE57CE7A

LastWrite: Thu Sep 10 21:40:41 2015

20150910 - Microsoft Visual Studio 2010 Tools for Office Runtime (x64) 10.0.50908 (Microsoft Corporation)

Key : 5149110B34767074BAD491825F8EF1DD

LastWrite: Tue Jan 19 22:17:55 2016

20160119 - TurboTax 2015 WinPerReleaseEngine 015.000.0423 (Intuit Inc.)

Key : 6414876250E69FF3395387C6C7F05BEB

LastWrite: Mon Dec 21 11:42:46 2015

20160310 - Microsoft .NET Framework 4.5.2 4.5.51209 (Microsoft Corporation)

Key : 717B20927FEB4444EB82C4359F203B2B

LastWrite: Sat Feb 20 01:50:09 2016

20160219 - Videograbber 1.0.0.0 (Freetec)

Key : 7C43C21609E58D74B9C5F017D78D7262

LastWrite: Thu Sep 10 18:41:27 2015

20150910 - swMSM 12.0.0.1 (Adobe Systems, Inc)

Key : 8BAD244577171E94B822900A94AE9569

LastWrite: Fri Feb 20 17:12:44 2015

20150220 - Renesas Electronics USB 3.0 Host Controller Driver 2.1.36.0 (Renesas Electronics Corporation)

Key : 8BFDDDD6597F70844985D521E5FA22BF8

LastWrite: Thu Jan 7 22:11:08 2016

20160107 - Bonjour 3.1.0.1 (Apple Inc.)

Key : 8F89BEBF4E463AF41AE5A4F924FF69E2

LastWrite: Thu Jan 7 22:40:42 2016

20160107 - iTunes 12.3.2.35 (Apple Inc.)

Key : 93BAD29AC2E44034A96BCB446EB8552E

LastWrite: Sat Feb 20 01:46:27 2016

## SOFTWARE OUTPUT

20160219 - Consumer Input Update Helper 1.3.25.309 (Compete Inc.)

Key : 9eab5ec6ac3d99b498a1d16c1c815acf

LastWrite: Tue Feb 2 00:14:47 2016

20160201 - Microsoft Visual C++ 2005 Redistributable (x64) 8.0.59192 (Microsoft Corporation)

Key : A089CE062ADB6BC44A720BA745894BAC

LastWrite: Thu Feb 4 14:19:10 2016

20160204 - Google Update Helper 1.3.29.5 (Google Inc.)

Key : AF057718A6CED58499106038EAF6DF1F

LastWrite: Wed Jan 13 23:15:11 2016

20160113 - Google Earth 7.1.5.1557 (Google)

Key : BE03F1969009A5748B9A1EFB9395F85D

LastWrite: Thu Jan 7 22:10:10 2016

20160107 - Apple Application Support (64-bit) 4.1.2 (Apple Inc.)

Key : c1c4f01781cc94c4c8fb1542c0981a2a

LastWrite: Thu Sep 10 19:09:17 2015

20150910 - Microsoft Visual C++ 2005 Redistributable 8.0.61001 (Microsoft Corporation)

Key : CCAAC517B97513845A4F8AA3D83EFE2E

LastWrite: Tue Feb 2 00:22:42 2016

20160201 - PaperPort Image Printer 64-bit 14.00.0000 (Nuance Communications, Inc.)

Key : CDBF5B88D769F1B42B199382A41E2210

LastWrite: Tue Feb 2 00:19:36 2016

20160201 - Nuance PaperPort 12 12.1.0005 (Nuance Communications, Inc.)

Key : D5591CDB6D837474B8A02B7BFCAEE1D7

LastWrite: Tue Jan 19 22:20:10 2016

20160119 - TurboTax 2015 WinPerTaxSupport 015.000.0175 (Intuit Inc.)

Key : D7314F9862C648A4DB8BE2A5B47BE100

LastWrite: Mon Dec 1 14:33:05 2014

20160114 - Microsoft Silverlight 5.1.41212.0 (Microsoft Corporation)

Key : DE818FF6F56855C40A37DDC6C97E6B8A

LastWrite: Tue Jan 19 22:16:20 2016

20160119 - TurboTax 2015 wrapper 015.000.0126 (Intuit Inc.)

Key : E1810453A043A7E44B90136643272B7F

LastWrite: Thu Jan 7 22:10:49 2016

20160107 - Apple Mobile Device Support 9.1.0.6 (Apple Inc.)

## SOFTWARE OUTPUT

Key : E1BEEC08C6A09B543A21731A2DF5EDCB

LastWrite: Thu Jan 7 22:07:26 2016

20160107 - QuickTime 7 7.78.80.95 (Apple Inc.)

Key : E547A84BA97BF714785724E14FC4291D

LastWrite: Tue Jan 19 22:20:17 2016

20160119 - TurboTax 2015 WinPerFuegoContent 015.000.0355 (Intuit Inc.)

Key : F5FE07CA6400DF84A99D787C11EC9B49

LastWrite: Tue Jan 19 23:15:19 2016

20160206 - TurboTax 2015 wmdiper 015.000.1163 (Intuit Inc.)

Key : FC03D219E93F13B4DAA921C3B697E42E

LastWrite: Wed Sep 16 04:30:09 2015

20150916 - HP Update 5.005.002.002 (Hewlett-Packard)

Key : FCCE9AF7ED2A1AD4FB3F1862D0DB6AF8

LastWrite: Thu Jan 7 22:09:15 2016

20160107 - Apple Application Support (32-bit) 4.1.2 (Apple Inc.)

User SID: S-1-5-21-3944275416-1635498007-1700510902-1000

Key : 23A5646B9EB883B4DA5CB4B4DD1CB0D0

LastWrite: Wed Sep 23 13:54:38 2015

20150923 - HPDiagnosticAlert 1.00.0001 (Microsoft)

Key : DA9AF51401ADEBA4796B05154D97C509

LastWrite: Wed Sep 23 13:54:35 2015

20150923 - HP FWUpdateED02 1.2.0.0 (Hewlett-Packard)

-----  
kb950582 v.20081212

(Software) KB950582 - Gets autorun settings from HKLM hive

NoDriveTypeAutoRun value may not exist: Can't call method "get\_data" on an undefined value at C:\Users\mdickson\Desktop\Tools\rrv2.8\plugins\kb950582.pl line 71.

HonorAutorunSetting not found.

Autorun settings in the HKLM hive take precedence over those in the HKCU hive.

-----  
LANDesk\ManagementSuite\WinClient\SoftwareMonitoring\MonitorLog not found.

Wow6432Node\LANDesk\ManagementSuite\WinClient\SoftwareMonitoring\MonitorLog not found.

LANDesk\Inventory\LogonHistory\Logons not found.

Wow6432Node\LANDesk\Inventory\LogonHistory\Logons not found.

-----  
macaddr v.20090118



## SOFTWARE OUTPUT

(Software) --

Microsoft\Windows Genuine Advantage not found.

-----

mrt v.20080804

(Software) Check to see if Malicious Software Removal Tool has been run

Key Path: Microsoft\RemovalTools\MRT

LastWrite Time Wed Apr 13 11:36:08 2016 (UTC)

Version: 6F31010B-5919-41C2-94FB-E71E8EEE9C9A

Analysis Tip: Go to <http://support.microsoft.com/kb/891716/> to see when MRT was last run. According to the KB article, each time MRT is run, a new GUID is written to the Version value.

-----

msis v.20090911

(Software) Determine MSI packages installed on the system

Classes\Installer\Products

LastWrite Time Sun Feb 21 01:16:17 2016 (UTC)

Wed Apr 20 15:01:53 2016 (UTC)

Microsoft Office Professional Plus 2010;C:\MSOCache\All  
Users\{90140000-0011-0000-0000-00000000FF1CE}-C\ProPlusWW.msi

Wed Apr 20 14:59:18 2016 (UTC)

Microsoft Silverlight;c:\7b77a2156d89ac7db8abc3d7\silverlight.msi

Wed Apr 20 14:56:14 2016 (UTC)

Adobe Flash Player 21 ActiveX;install\_flash\_player\_21\_active\_x.msi

Wed Apr 20 14:56:02 2016 (UTC)

Adobe Flash Player 21 NPAPI;install\_flash\_player\_21\_plugin.msi

Wed Apr 20 13:37:20 2016 (UTC)

Microsoft .NET Framework 4 Extended;C:\WINDOWS\TEMP\Microsoft .NET Framework 4  
Setup\_4.0.30319\netfx\_Extended\_x64.msi

Wed Apr 20 13:36:48 2016 (UTC)

Microsoft .NET Framework 4 Client Profile;C:\WINDOWS\TEMP\Microsoft .NET Framework  
4 Setup\_4.0.30319\netfx\_Core\_x64.msi

Wed Apr 20 13:20:08 2016 (UTC)

McAfee Agent;MFEagent\_x64.msi

Wed Apr 20 13:00:14 2016 (UTC)

WebEx Training Manager for Firefox or  
Chrome;C:\WINDOWS\ccmcache\3\Training\_Center\attcns\_firefox.msi

Wed Apr 20 12:59:59 2016 (UTC)

Cisco WebEx Meeting Center for Firefox or  
Chrome;C:\WINDOWS\ccmcache\3\Mtg\_Center\atmcns\_firefox.msi

Wed Apr 20 12:59:43 2016 (UTC)

WebEx Event Manager for Firefox or

## SOFTWARE OUTPUT

Chrome;C:\WINDOWS\ccmcache\3\Event\_Center\atecns\_firefox.msi  
 Wed Apr 20 12:59:26 2016 (UTC)  
 Google Chrome;googlechromestandaloneenterprise.msi  
 Tue Apr 19 20:55:59 2016 (UTC)  
 GlobalSubmit Review 2014;Review.msi  
 Tue Apr 19 20:52:00 2016 (UTC)  
 Google Update Helper;C:\Program Files  
 (x86)\Google\Update\1.3.29.5\GoogleUpdateHelper.msi  
 Tue Apr 19 20:41:24 2016 (UTC)  
 Cisco Jabber;CiscoJabberSetup.msi  
 Tue Apr 19 20:40:20 2016 (UTC)  
 Cisco IP Communicator;CiscoIPCommunicatorSetup.msi  
 Tue Apr 19 20:00:03 2016 (UTC)  
 Configuration Manager  
 Client;C:\WINDOWS\ccmsetup\{72875A95-4007-4DAC-88D8-66366F9A5045}\client.msi  
 Mon Apr 18 16:27:08 2016 (UTC)  
 Adobe Refresh Manager;C:\Program Files (x86)\Common  
 Files\Adobe\ARM\1.0\Cache\Arm\_001824166751\_84172875934957120440285551113286767.msi  
 Mon Apr 18 16:02:28 2016 (UTC)  
 McAfee Host Intrusion  
 Prevention;C:\\_SMSTaskSequence\Packages\PS1002F3\McAfeeHIP\_ClientSetup\_X64.msi  
 Mon Apr 18 16:00:10 2016 (UTC)  
 Microsoft Visual C++ 2010 x64 Redistributable -  
 10.0.40219;C:\3cb5f26f2fc5f9d5c4e783d5be\vc\_red.msi  
 Mon Apr 18 16:00:05 2016 (UTC)  
 Microsoft Visual C++ 2010 x86 Redistributable -  
 10.0.40219;C:\dac6f6cbcef6992dde8507\vc\_red.msi  
 Mon Apr 18 15:58:41 2016 (UTC)  
 McAfee VirusScan Enterprise;VSE880.MSI  
 Mon Apr 18 15:57:46 2016 (UTC)  
 Check Point Endpoint Security - Full Disk Encryption;Pointsec for PC.msi  
 Mon Apr 18 15:57:15 2016 (UTC)  
 Cisco Systems VPN Client  
 5.0.07.0440;C:\\_SMSTaskSequence\Packages\FDA00080\5.0.07.0440\vpnclient\_setup.msi  
 Mon Apr 18 15:56:55 2016 (UTC)  
 Cisco AnyConnect Start Before Login  
 Module;C:\\_SMSTaskSequence\Packages\FDA002D5\anyconnect-gina-win-3.1.05160-pre-deplo  
 y-k9.msi  
 Mon Apr 18 15:56:54 2016 (UTC)  
 Cisco AnyConnect Secure Mobility  
 Client;C:\\_SMSTaskSequence\Packages\FDA002D5\anyconnect-win-3.1.05160-pre-deploy-k9.  
 msi  
 Cisco AnyConnect Diagnostics and Reporting  
 Tool;C:\\_SMSTaskSequence\Packages\FDA002D5\anyconnect-dart-win-3.1.05160-k9.msi  
 Mon Apr 18 15:54:53 2016 (UTC)  
 WebEx Productivity  
 Tools;C:\\_SMSTaskSequence\Packages\PS1002D1\Productivity\_Tools\ptools.msi  
 Mon Apr 18 15:54:47 2016 (UTC)

## SOFTWARE OUTPUT

WebEx Document  
Suite;C:\\_SMSTaskSequence\Packages\PS1002D1\Productivity\_Tools\atucfsuite.msi  
Mon Apr 18 15:54:46 2016 (UTC)

WebEx Support Manager for Internet  
Explorer;C:\\_SMSTaskSequence\Packages\PS1002D1\Support\_Center\SC\_Win.msi  
Mon Apr 18 15:54:44 2016 (UTC)

WebEx Training Manager for Internet  
Explorer;C:\\_SMSTaskSequence\Packages\PS1002D1\Training\_Center\attcie\_ie.msi  
Mon Apr 18 15:54:43 2016 (UTC)

Network Recording  
Player;C:\\_SMSTaskSequence\Packages\PS1002D1\Players\ARF\_nbr2player.msi  
Mon Apr 18 15:54:42 2016 (UTC)

Cisco WebEx Meeting Center for Internet  
Explorer;C:\\_SMSTaskSequence\Packages\PS1002D1\Mtg\_Center\atmcie\_ie.msi  
Mon Apr 18 15:54:40 2016 (UTC)

WebEx Poll Questionnaire  
Editor;C:\\_SMSTaskSequence\Packages\PS1002D1\Event\_Center\polleditor.msi  
Mon Apr 18 15:54:39 2016 (UTC)

WebEx Event Manager for Internet  
Explorer;C:\\_SMSTaskSequence\Packages\PS1002D1\Event\_Center\atecie\_ie.msi  
Mon Apr 18 15:54:25 2016 (UTC)

Java(TM) 6 Update  
38;C:\WINDOWS\SysWOW64\config\systemprofile\AppData\LocalLow\Sun\Java\jre1.6.0\_38\jre1.6.0\_38.msi  
Mon Apr 18 15:54:19 2016 (UTC)

SAFE Servlet;C:\\_SMSTaskSequence\Packages\PS10004B\Encase\Setup.msi  
Mon Apr 18 15:54:07 2016 (UTC)

Java(TM) 6 Update 17;C:\\_SMSTaskSequence\Packages\FDA0004E\jre1.6.0\_17.msi  
Mon Apr 18 15:45:54 2016 (UTC)

WinZip 17.5;C:\\_SMSTaskSequence\Packages\FDA0022E\winzip175-64.msi  
Mon Apr 18 15:45:32 2016 (UTC)

ActivClient x64;Z:\Applications\ActivClient(6.2.0.179)\ActivClient x64 6.2.msi  
Mon Apr 18 15:44:52 2016 (UTC)

Adobe Acrobat X Pro;C:\\_SMSTaskSequence\Packages\FDA000C7\Adobe Acrobat X\AcroPro.msi  
Mon Apr 18 15:37:43 2016 (UTC)

DisplayLink Graphics;C:\\_SMSTaskSequence\Packages\PS1002C3\Setup.msi  
Mon Apr 18 15:37:38 2016 (UTC)

DisplayLink Core  
Software;C:\\_SMSTaskSequence\Packages\PS1002C3\DisplayLinkCore.msi  
Mon Apr 18 15:30:46 2016 (UTC)

Microsoft Policy Platform;C:\WINDOWS\ccmsetup\MicrosoftPolicyPlatformSetup.msi  
Mon Apr 18 15:30:43 2016 (UTC)

Microsoft Visual C++ 2005 Redistributable  
(x64);C:\WINDOWS\TEMP\IXP000.TMP\vc redistrib.msi  
Mon Apr 18 15:30:36 2016 (UTC)

Microsoft Visual C++ 2013 x86 Additional Runtime -  
12.0.21005;C:\ProgramData\Package

## SOFTWARE OUTPUT

Cache\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}\v12.0.21005\packages\vcRuntimeAdditional\_x86\vc\_runtimeAdditional\_x86.msi  
 Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005;C:\ProgramData\Package  
 Cache\{929FBD26-9020-399B-9A7A-751D61F0B942}\v12.0.21005\packages\vcRuntimeAdditional\_amd64\vc\_runtimeAdditional\_x64.msi  
 Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005;C:\ProgramData\Package  
 Cache\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}\v12.0.21005\packages\vcRuntimeMinimum\_amd64\vc\_runtimeMinimum\_x64.msi  
 Mon Apr 18 15:30:35 2016 (UTC)  
 Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005;C:\ProgramData\Package  
 Cache\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\v12.0.21005\packages\vcRuntimeMinimum\_x86\vc\_runtimeMinimum\_x86.msi  
 Mon Apr 18 15:28:10 2016 (UTC)  
 Realtek Audio COM Components;C:\Program Files\Realtek\Audio\HDA\SetupRAPCOM.msi  
 Wed Apr 13 11:38:25 2016 (UTC)  
 Microsoft Office Outlook 2010;C:\MSOCache\All  
 Users\{90140000-001A-0000-0000-0000000FF1CE}-C\OutlookWW.msi  
 Wed Apr 13 11:37:12 2016 (UTC)  
 Microsoft Office Home and Student 2007;C:\MSOCache\All  
 Users\{91120000-002F-0000-0000-0000000FF1CE}-C\HomeStudentrWW.msi  
 Thu Mar 10 13:44:09 2016 (UTC)  
 Microsoft .NET Framework 4.5.2;netfx\_Full\_GDR\_x64.msi  
 Thu Mar 10 13:37:50 2016 (UTC)  
 Microsoft Office Office 64-bit Components 2010;C:\MSOCache\All  
 Users\{90140000-001A-0000-0000-0000000FF1CE}-C\Office64WW.msi  
 Sat Feb 20 01:50:09 2016 (UTC)  
 Videograbber;C:\ProgramData\Package  
 Cache\{2902B717-BEF7-4444-BE28-4C53F902B3B2}\v1.0.0.0\videograbber\_Setup\_product-website\_en-US.msi  
 Tue Feb 9 22:20:38 2016 (UTC)  
 Microsoft Office Outlook MUI (English) 2010;C:\MSOCache\All  
 Users\{90140000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.msi  
 Sat Feb 6 19:50:38 2016 (UTC)  
 TurboTax 2015 WinPerFedFormset;D:\TurboTax 2015\MSI\WinPerFedFormset.msi  
 Sat Feb 6 19:50:27 2016 (UTC)  
 TurboTax 2015 wmdiper;C:\ProgramData\Intuit\Common\Update  
 Service\v4\Data\b011941567434707ab4d1928f5e81fdd\C\C-wmdiper\015.000.1121\_msi\v1\F\wmdiper.msi  
 Thu Feb 4 20:02:22 2016 (UTC)  
 Microsoft Visual C++ 2005 Redistributable (x64);C:\Windows\TEMP\IXP000.TMP\vcredist.msi  
 Thu Feb 4 20:01:57 2016 (UTC)  
 MSXML 4.0 SP3 Parser (KB2758694);c:\e79bd3a44165fa5fbf27110e88a20a84\msxml.msi  
 Thu Feb 4 14:19:10 2016 (UTC)  
 Google Update Helper;C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleUpdateHelper.msi  
 Tue Feb 2 00:22:42 2016 (UTC)

## SOFTWARE OUTPUT

PaperPort Image Printer 64-bit;D:\paperport\PPImgPrinter\System64\PaperPort Image Printer 64-bit.msi  
 Tue Feb 2 00:21:29 2016 (UTC)  
 Nuance PDF Viewer Plus;D:\paperport\PDFViewer\PDFViewer\Nuance PDF Viewer Plus.msi  
 Tue Feb 2 00:21:28 2016 (UTC)  
 Scansoft PDF Professional;  
 Tue Feb 2 00:19:37 2016 (UTC)  
 Nuance PaperPort 12;D:\paperport\PaperPort\Nuance PaperPort 12.msi  
 Tue Feb 2 00:14:47 2016 (UTC)  
 Microsoft Visual C++ 2005 Redistributable  
 (x64);C:\Users\ABE-AR~1\AppData\Local\Temp\IXP000.TMP\vc redistrib.msi  
 Tue Feb 2 00:11:50 2016 (UTC)  
 Microsoft Visual C++ 2005  
 Redistributable;C:\Users\ABE-AR~1\AppData\Local\Temp\IXP000.TMP\vc redistrib.msi  
 Tue Feb 2 00:09:45 2016 (UTC)  
 MSXML 4.0 SP3 Parser;D:\paperport\Prerequisite\Msxml4-SP3.msi  
 Tue Jan 19 22:39:08 2016 (UTC)  
 TurboTax 2015 WinPerFuegoContent;D:\TurboTax 2015\MSI\WinPerFuegoContent.msi  
 Tue Jan 19 22:36:17 2016 (UTC)  
 TurboTax 2015 WinPerTaxSupport;D:\TurboTax 2015\MSI\WinPerTaxSupport.msi  
 Tue Jan 19 22:34:36 2016 (UTC)  
 TurboTax 2015 WinPerReleaseEngine;D:\TurboTax 2015\MSI\WinPerReleaseEngine.msi  
 Tue Jan 19 22:16:20 2016 (UTC)  
 TurboTax 2015 wrapper;D:\TurboTax 2015\MSI\wrapper.msi  
 Thu Jan 14 16:38:04 2016 (UTC)  
 Microsoft Silverlight;c:\42296d043a65c868120701\silverlight.msi  
 Wed Jan 13 23:15:11 2016 (UTC)  
 Google Earth;C:\Users\ABE-AR~1\AppData\Local\Temp\GE1669.tmp  
 Thu Jan 7 22:15:30 2016 (UTC)  
 iTunes;C:\Users\Abe-Arjun Malik\AppData\Local\Apple\Apple Software  
 Update\iTunes6464.msi  
 Thu Jan 7 22:11:08 2016 (UTC)  
 Bonjour;C:\Users\Abe-Arjun Malik\AppData\Local\Apple\Apple Software  
 Update\Bonjour64.msi  
 Thu Jan 7 22:10:50 2016 (UTC)  
 Apple Mobile Device Support;C:\Users\Abe-Arjun Malik\AppData\Local\Apple\Apple  
 Software Update\AppleMobileDeviceSupport6464.msi  
 Thu Jan 7 22:10:30 2016 (UTC)  
 Apple Software Update;C:\Users\Abe-Arjun Malik\AppData\Local\Apple\Apple Software  
 Update\AppleSoftwareUpdate.msi  
 Thu Jan 7 22:10:10 2016 (UTC)  
 Apple Application Support (64-bit);C:\Users\Abe-Arjun  
 Malik\AppData\Local\Apple\Apple Software Update\AppleApplicationSupport64.msi  
 Thu Jan 7 22:09:15 2016 (UTC)  
 Apple Application Support (32-bit);C:\Users\Abe-Arjun  
 Malik\AppData\Local\Apple\Apple Software Update\AppleApplicationSupport.msi  
 Thu Jan 7 22:07:26 2016 (UTC)  
 QuickTime 7;C:\Users\Abe-Arjun Malik\AppData\Local\Apple\Apple Software

## SOFTWARE OUTPUT

Update\QuickTime.msi  
 Wed Dec 30 12:33:34 2015 (UTC)  
 Microsoft Visual C++ 2005 Redistributable;C:\WINDOWS\TEMP\IXP000.TMP\vc redistrib.msi  
 Wed Dec 30 12:24:53 2015 (UTC)  
 EMC SourceOne Offline Access;C:\windows\Downloaded  
 Installations\{8E968E35-FC28-4D31-98CB-E6152C341C97}\ES1\_OfflineAccess.msi  
 Wed Dec 30 12:23:41 2015 (UTC)  
 Citrix online plug-in  
 (HDX);C:\Users\ADMINI~1\AppData\Local\Temp\Ctx-4669FF88-1230-4B04-9E12-04A8A4DC9FCE\  
 Extract\CitrixHDXMediaStreamForFlash-ClientInstall.msi  
 Wed Dec 30 12:23:40 2015 (UTC)  
 Citrix online plug-in  
 (DV);C:\Users\ADMINI~1\AppData\Local\Temp\Ctx-4669FF88-1230-4B04-9E12-04A8A4DC9FCE\  
 Extract\DesktopViewer.msi  
 Wed Dec 30 12:23:38 2015 (UTC)  
 Citrix online plug-in  
 (USB);C:\Users\ADMINI~1\AppData\Local\Temp\Ctx-4669FF88-1230-4B04-9E12-04A8A4DC9FCE\  
 Extract\GenericUSB.msi  
 Wed Dec 30 12:23:31 2015 (UTC)  
 Citrix online plug-in  
 (Web);C:\Users\ADMINI~1\AppData\Local\Temp\Ctx-4669FF88-1230-4B04-9E12-04A8A4DC9FCE\  
 Extract\ICAWebWrapper.msi  
 Wed Dec 30 12:23:18 2015 (UTC)  
 Access Card Utility;Z:\Applications\Access Card Utility  
 1.4.2\AccessCardUtilitySetup.msi  
 Wed Dec 30 12:20:19 2015 (UTC)  
 eRoom 7  
 Client;C:\Users\ADMINI~1\AppData\Local\Temp\{CD8C4F5A-FA28-4C9C-B8E0-8FDCAC57609D}\e  
 Room7Client.msi  
 Wed Dec 30 10:06:56 2015 (UTC)  
 Microsoft Office Proof (English) 2010;C:\MSOCache\All  
 Users\{90140000-002C-0409-0000-00000000FF1CE}-C\Proof.en\Proof.msi  
 Wed Dec 30 09:57:51 2015 (UTC)  
 Microsoft Office OneNote MUI (English) 2010;C:\MSOCache\All  
 Users\{90140000-00A1-0409-0000-00000000FF1CE}-C\OneNoteMUI.msi  
 Wed Dec 30 09:57:46 2015 (UTC)  
 Microsoft Office Office 64-bit Components 2010;C:\MSOCache\All  
 Users\{90140000-0011-0000-0000-00000000FF1CE}-C\Office64WW.msi  
 Wed Dec 30 09:55:56 2015 (UTC)  
 Microsoft Office Word MUI (English) 2010;C:\MSOCache\All  
 Users\{90140000-001B-0409-0000-00000000FF1CE}-C\WordMUI.msi  
 Wed Dec 30 09:55:53 2015 (UTC)  
 Microsoft Office Outlook MUI (English) 2010;C:\MSOCache\All  
 Users\{90140000-001A-0409-0000-00000000FF1CE}-C\OutlookMUI.msi  
 Wed Dec 30 09:55:13 2015 (UTC)  
 Microsoft Office Shared MUI (English) 2010;C:\MSOCache\All  
 Users\{90140000-0115-0409-0000-00000000FF1CE}-C\OfficeMUI.msi  
 Wed Dec 30 08:44:57 2015 (UTC)

## SOFTWARE OUTPUT

Microsoft Office PowerPoint MUI (English) 2010;C:\MSOCache\All  
Users\{90140000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.msi  
Wed Dec 30 08:44:54 2015 (UTC)

Microsoft Office Excel MUI (English) 2010;C:\MSOCache\All  
Users\{90140000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.msi  
Wed Dec 30 08:42:54 2015 (UTC)

Microsoft Office Proof (Spanish) 2010;C:\MSOCache\All  
Users\{90140000-002C-0409-0000-0000000FF1CE}-C\Proof.es\Proof.msi  
Wed Dec 30 08:42:51 2015 (UTC)

Microsoft Office Proof (French) 2010;C:\MSOCache\All  
Users\{90140000-002C-0409-0000-0000000FF1CE}-C\Proof.fr\Proof.msi  
Wed Dec 30 07:06:36 2015 (UTC)

Microsoft Lync 2010;C:\Program Files (x86)\OCSetup\Lync.msi  
Wed Dec 30 00:26:49 2015 (UTC)

Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2010;C:\MSOCache\All  
Users\{90140000-0116-0409-1000-0000000FF1CE}-C\Office64MUISet.msi  
Wed Dec 30 00:26:47 2015 (UTC)

Microsoft Office Shared 64-bit MUI (English) 2010;C:\MSOCache\All  
Users\{90140000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.msi  
Wed Dec 30 00:26:28 2015 (UTC)

Microsoft Office Publisher MUI (English) 2010;C:\MSOCache\All  
Users\{90140000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.msi  
Wed Dec 30 00:26:25 2015 (UTC)

Microsoft Office Proofing (English) 2010;C:\MSOCache\All  
Users\{90140000-002C-0409-0000-0000000FF1CE}-C\Proofing.msi  
Wed Dec 30 00:26:12 2015 (UTC)

Microsoft Office Shared Setup Metadata MUI (English) 2010;C:\MSOCache\All  
Users\{90140000-0115-0409-0000-0000000FF1CE}-C\OfficeMUISet.msi  
Wed Dec 30 00:26:06 2015 (UTC)

Microsoft Office InfoPath MUI (English) 2010;C:\MSOCache\All  
Users\{90140000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.msi  
Wed Dec 30 00:26:02 2015 (UTC)

Microsoft Office Groove MUI (English) 2010;C:\MSOCache\All  
Users\{90140000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.msi  
Wed Dec 30 00:25:55 2015 (UTC)

Microsoft Office Access Setup Metadata MUI (English) 2010;C:\MSOCache\All  
Users\{90140000-0117-0409-0000-0000000FF1CE}-C\AccessMUISet.msi  
Wed Dec 30 00:25:52 2015 (UTC)

Microsoft Office Access MUI (English) 2010;C:\MSOCache\All  
Users\{90140000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\AccessMUI.msi  
Tue Dec 29 22:29:49 2015 (UTC)

Microsoft Visual Studio 2010 Tools for Office Runtime  
(x64);c:\ffcf0de99483c3b8404d06720ece77548\vstor40\_x64.msi  
Tue Dec 29 18:27:34 2015 (UTC)

Microsoft Visual C++ 2008 Redistributable - x86  
9.0.30729.6161;c:\7bfee4305bf8ac2d04340f06\vc\_red.msi  
Tue Dec 29 18:26:52 2015 (UTC)

Microsoft Visual C++ 2008 Redistributable - x64

## SOFTWARE OUTPUT

9.0.30729.6161;c:\f0f7a84a229330edc7\vc\_red.msi

Tue Dec 29 16:08:46 2015 (UTC)

Microsoft Office Live Meeting 2007;Z:\Applications\Microsoft Office Live Meeting 2007\LMConsole.msi

Tue Dec 29 16:06:55 2015 (UTC)

Microsoft Visual C++ 2008 Redistributable - x64

9.0.30729.4148;c:\d6a21fa13028cb2bd6c663889fb6be\vc\_red.msi

Tue Dec 29 16:05:49 2015 (UTC)

Microsoft Visual C++ 2008 Redistributable - x86

9.0.30729.4148;c:\01cb7e3f01e8447dcd8b\vc\_red.msi

Wed Nov 11 22:05:10 2015 (UTC)

Microsoft Office Shared MUI (English) 2010;C:\MSOCache\All Users\{90140000-0115-0409-0000-00000000FF1CE}-C\OfficeMUI.msi

Wed Nov 11 22:04:39 2015 (UTC)

Microsoft Office Shared MUI (English) 2007;C:\MSOCache\All Users\{90120000-0115-0409-0000-00000000FF1CE}-C\OfficeMUI.msi

Wed Sep 16 04:30:09 2015 (UTC)

HP Update;C:\Users\Abe-Arjun Malik\AppData\Local\Temp\7zS6C84\Optional\HP Update.msi

Thu Sep 10 23:33:01 2015 (UTC)

Microsoft Office Outlook Connector;C:\Program Files (x86)\MSECache\OlkConnector\olc.msi

Thu Sep 10 22:17:48 2015 (UTC)

Microsoft Office Proof (Spanish) 2010;C:\MSOCache\All Users\{90140000-002C-0409-0000-00000000FF1CE}-C\Proof.es\Proof.msi

Thu Sep 10 22:17:45 2015 (UTC)

Microsoft Office Proof (French) 2010;C:\MSOCache\All Users\{90140000-002C-0409-0000-00000000FF1CE}-C\Proof.fr\Proof.msi

Thu Sep 10 22:17:42 2015 (UTC)

Microsoft Office Proof (English) 2010;C:\MSOCache\All Users\{90140000-002C-0409-0000-00000000FF1CE}-C\Proof.en\Proof.msi

Thu Sep 10 21:45:17 2015 (UTC)

Microsoft Office File Validation Add-In;OFV.msi

Thu Sep 10 21:45:04 2015 (UTC)

Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2010;C:\MSOCache\All Users\{90140000-0116-0409-1000-00000000FF1CE}-C\Office64MUISet.msi

Thu Sep 10 21:45:01 2015 (UTC)

Microsoft Office Shared 64-bit MUI (English) 2010;C:\MSOCache\All Users\{90140000-0116-0409-1000-00000000FF1CE}-C\Office64MUI.msi

Thu Sep 10 21:44:48 2015 (UTC)

Microsoft Office Proofing (English) 2010;C:\MSOCache\All Users\{90140000-002C-0409-0000-00000000FF1CE}-C\Proofing.msi

Thu Sep 10 21:42:53 2015 (UTC)

Microsoft Office Shared Setup Metadata MUI (English) 2010;C:\MSOCache\All Users\{90140000-0115-0409-0000-00000000FF1CE}-C\OfficeMUISet.msi

Thu Sep 10 21:40:41 2015 (UTC)

Microsoft Visual Studio 2010 Tools for Office Runtime (x64);c:\0574c3a2e23186e2e757b2fe31d8\vstor40\_x64.msi



## SOFTWARE OUTPUT

Thu Sep 10 21:40:31 2015 (UTC)

Microsoft Visual C++ 2010 x64 Redistributable -  
10.0.40219;c:\4e3e0ac048cc2f170825ca9b90aeb7\VC\_Red\_x64\vc\_red.msi

Thu Sep 10 21:40:26 2015 (UTC)

Microsoft Visual C++ 2010 x86 Redistributable -  
10.0.40219;c:\4e3e0ac048cc2f170825ca9b90aeb7\VC\_Red\_x86\vc\_red.msi

Thu Sep 10 21:08:23 2015 (UTC)

Microsoft Office Office 64-bit Components 2007;C:\MSOCache\All  
Users\{91120000-002F-0000-0000-00000000FF1CE}-C\Office64WW.msi

Thu Sep 10 19:42:26 2015 (UTC)

Microsoft Office OneNote MUI (English) 2007;C:\MSOCache\All  
Users\{90120000-00A1-0409-0000-00000000FF1CE}-C\OneNoteMUI.msi

Thu Sep 10 19:26:55 2015 (UTC)

Microsoft Office PowerPoint MUI (English) 2007;C:\MSOCache\All  
Users\{90120000-0018-0409-0000-00000000FF1CE}-C\PowerPointMUI.msi

Thu Sep 10 19:21:49 2015 (UTC)

Microsoft Office Word MUI (English) 2007;C:\MSOCache\All  
Users\{90120000-001B-0409-0000-00000000FF1CE}-C\WordMUI.msi

Thu Sep 10 19:19:37 2015 (UTC)

Microsoft Office Excel MUI (English) 2007;C:\MSOCache\All  
Users\{90120000-0016-0409-0000-00000000FF1CE}-C\ExcelMUI.msi

Thu Sep 10 19:16:21 2015 (UTC)

Microsoft Office Proof (French) 2007;C:\MSOCache\All  
Users\{90120000-002C-0409-0000-00000000FF1CE}-C\Proof.fr\Proof.msi

Thu Sep 10 19:16:17 2015 (UTC)

Microsoft Office Proof (Spanish) 2007;C:\MSOCache\All  
Users\{90120000-002C-0409-0000-00000000FF1CE}-C\Proof.es\Proof.msi

Thu Sep 10 19:16:13 2015 (UTC)

Microsoft Office Proof (English) 2007;C:\MSOCache\All  
Users\{90120000-002C-0409-0000-00000000FF1CE}-C\Proof.en\Proof.msi

Thu Sep 10 19:12:19 2015 (UTC)

Microsoft Office Shared Setup Metadata MUI (English) 2007;C:\MSOCache\All  
Users\{90120000-0115-0409-0000-00000000FF1CE}-C\OfficeMUISet.msi

Thu Sep 10 19:12:16 2015 (UTC)

Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2007;C:\MSOCache\All  
Users\{90120000-0116-0409-1000-00000000FF1CE}-C\Office64MUISet.msi

Thu Sep 10 19:12:07 2015 (UTC)

Microsoft Office Shared 64-bit MUI (English) 2007;C:\MSOCache\All  
Users\{90120000-0116-0409-1000-00000000FF1CE}-C\Office64MUI.msi

Thu Sep 10 19:09:17 2015 (UTC)

Microsoft Visual C++ 2005  
Redistributable;C:\Users\ABE-AR~1\AppData\Local\Temp\IXP000.TMP\vc\_redist.msi

Thu Sep 10 18:41:27 2015 (UTC)

swMSM;C:\Windows\SysWOW64\Adobe\Shockwave 12\swMSM.msi

Thu Sep 10 16:31:32 2015 (UTC)

Microsoft Office Proofing (English) 2007;C:\MSOCache\All  
Users\{90120000-002C-0409-0000-00000000FF1CE}-C\Proofing.msi

Fri Feb 20 17:12:44 2015 (UTC)

## SOFTWARE OUTPUT

Renesas Electronics USB 3.0 Host Controller Driver;C:\drivers\sp54511\nusb3drv.msi  
 Fri Feb 20 17:05:34 2015 (UTC)

Validity Fingerprint Sensor Driver;C:\Windows\Installer\HPVFSSVC4.5.133.0.msi

-----  
 networkcards v.20080325  
 (Software) Get NetworkCards

NetworkCards  
 Microsoft\Windows NT\CurrentVersion\NetworkCards

Intel(R) 82579LM Gigabit Network Connection [Fri Feb 20 16:53:44 2015]  
 Intel(R) Centrino(R) Advanced-N 6205 [Fri Feb 20 18:22:36 2015]  
 Apple Mobile Device Ethernet [Sat Nov 28 20:21:44 2015]  
 Intel(R) Centrino(R) Ultimate-N 6300 AGN [Thu Sep 3 17:49:38 2015]  
 Intel(R) Centrino(R) Advanced-N 6205 [Fri Feb 20 16:53:49 2015]  
 -----

Launching networklist v.20141204  
 (Software) Collects network info from Vista+ NetworkList key

Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles  
 Network

Key LastWrite : Thu Sep 3 17:49:10 2015 UTC  
 DateLastConnected: Thu Sep 3 10:49:10 2015  
 DateCreated : Fri Feb 20 10:44:25 2015  
 DefaultGatewayMac: 00-00-5E-00-01-03  
 Type : wired  
 Category : Private

Braddock  
 Key LastWrite : Wed Apr 20 09:07:04 2016 UTC  
 DateLastConnected: Wed Apr 20 05:07:04 2016  
 DateCreated : Thu Sep 10 10:03:48 2015  
 DefaultGatewayMac: E0-3F-49-9A-7B-40  
 Type : wireless  
 Category : Private

Abe-Arjun's iPhone (2)  
 Key LastWrite : Sun Mar 13 00:22:56 2016 UTC  
 DateLastConnected: Sat Mar 12 19:22:56 2016  
 DateCreated : Sat Sep 26 12:14:44 2015  
 DefaultGatewayMac: 7A-D7-5F-C0-B9-64  
 Type : wireless  
 Category : Private

-----  
 networkuid v.20100312  
 (Software) Gets Network key UID value

## SOFTWARE OUTPUT

Microsoft\Windows NT\CurrentVersion\Network not found.

-----  
product v.20100325

(Software) Get installed product info

Microsoft\Windows\CurrentVersion\Installer\UserData

S-1-5-18

Wed Apr 13 11:38:24 2016 Z

Microsoft Office Outlook 2010 v.14.0.7015.1000, 20160413

Wed Apr 13 11:37:12 2016 Z

Microsoft Office Home and Student 2007 v.12.0.6612.1000, 20160413

Thu Mar 10 13:44:09 2016 Z

Microsoft .NET Framework 4.5.2 v.4.5.51209, 20160310

Thu Mar 10 13:37:50 2016 Z

Microsoft Office Office 64-bit Components 2010 v.14.0.7015.1000, 20160310

Sat Feb 20 01:50:09 2016 Z

Videograbber v.1.0.0.0, 20160219

Sat Feb 20 01:46:27 2016 Z

Consumer Input Update Helper v.1.3.25.309, 20160219

Tue Feb 9 22:20:38 2016 Z

Microsoft Office Outlook MUI (English) 2010 v.14.0.7015.1000, 20160209

Sat Feb 6 19:50:38 2016 Z

TurboTax 2015 WinPerFedFormset v.015.000.1781, 20160206

Sat Feb 6 19:50:27 2016 Z

TurboTax 2015 wmdiper v.015.000.1163, 20160206

Thu Feb 4 20:02:22 2016 Z

Microsoft Visual C++ 2005 Redistributable (x64) v.8.0.61000, 20160204

Thu Feb 4 20:01:56 2016 Z

MSXML 4.0 SP3 Parser (KB2758694) v.4.30.2117.0, 20160204

Thu Feb 4 14:19:10 2016 Z

Google Update Helper v.1.3.29.5, 20160204

Tue Feb 2 00:22:42 2016 Z

PaperPort Image Printer 64-bit v.14.00.0000, 20160201

Tue Feb 2 00:21:29 2016 Z

Nuance PDF Viewer Plus v.5.30.3290, 20160201

Tue Feb 2 00:19:36 2016 Z

Nuance PaperPort 12 v.12.1.0005, 20160201

Tue Feb 2 00:14:47 2016 Z

Microsoft Visual C++ 2005 Redistributable (x64) v.8.0.59192, 20160201

Tue Feb 2 00:11:50 2016 Z

Microsoft Visual C++ 2005 Redistributable v.8.0.59193, 20160201

Tue Feb 2 00:09:45 2016 Z

MSXML 4.0 SP3 Parser v.4.30.2100.0, 20160201

Tue Jan 19 22:39:08 2016 Z

TurboTax 2015 WinPerFuegoContent v.015.000.0355, 20160119

Tue Jan 19 22:36:17 2016 Z

## SOFTWARE OUTPUT

TurboTax 2015 WinPerTaxSupport v.015.000.0175, 20160119  
 Tue Jan 19 22:34:36 2016 Z  
 TurboTax 2015 WinPerReleaseEngine v.015.000.0423, 20160119  
 Tue Jan 19 22:16:20 2016 Z  
 TurboTax 2015 wrapper v.015.000.0126, 20160119  
 Thu Jan 14 16:38:03 2016 Z  
 Microsoft Silverlight v.5.1.41212.0, 20160114  
 Wed Jan 13 23:15:11 2016 Z  
 Google Earth v.7.1.5.1557, 20160113  
 Thu Jan 7 22:40:42 2016 Z  
 iTunes v.12.3.2.35, 20160107  
 Thu Jan 7 22:11:08 2016 Z  
 Bonjour v.3.1.0.1, 20160107  
 Thu Jan 7 22:10:49 2016 Z  
 Apple Mobile Device Support v.9.1.0.6, 20160107  
 Thu Jan 7 22:10:30 2016 Z  
 Apple Software Update v.2.1.4.131, 20160107  
 Thu Jan 7 22:10:10 2016 Z  
 Apple Application Support (64-bit) v.4.1.2, 20160107  
 Thu Jan 7 22:09:15 2016 Z  
 Apple Application Support (32-bit) v.4.1.2, 20160107  
 Thu Jan 7 22:07:26 2016 Z  
 QuickTime 7 v.7.78.80.95, 20160107  
 Wed Nov 11 22:05:10 2015 Z  
 Microsoft Office Shared MUI (English) 2010 v.14.0.7015.1000, 20151111  
 Wed Nov 11 22:04:38 2015 Z  
 Microsoft Office Shared MUI (English) 2007 v.12.0.6612.1000, 20151111  
 Wed Sep 16 04:30:09 2015 Z  
 HP Update v.5.005.002.002, 20150916  
 Fri Sep 11 15:59:34 2015 Z  
 Microsoft Office Proofing (English) 2010 v.14.0.7015.1000, 20150910  
 Fri Sep 11 15:59:32 2015 Z  
 Microsoft Office Proof (English) 2010 v.14.0.7015.1000, 20150910  
 Fri Sep 11 15:59:28 2015 Z  
 Microsoft Office Proof (French) 2010 v.14.0.7015.1000, 20150910  
 Fri Sep 11 15:59:24 2015 Z  
 Microsoft Office Proof (Spanish) 2010 v.14.0.7015.1000, 20150910  
 Fri Sep 11 15:59:21 2015 Z  
 Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2010 v.14.0.7015.1000, 20150910  
 Fri Sep 11 15:59:19 2015 Z  
 Microsoft Office Shared 64-bit MUI (English) 2010 v.14.0.7015.1000, 20150910  
 Fri Sep 11 15:59:11 2015 Z  
 Microsoft Office Shared Setup Metadata MUI (English) 2010 v.14.0.7015.1000, 20150910  
 Thu Sep 10 23:33:01 2015 Z  
 Microsoft Office Outlook Connector v.14.0.6123.5001, 20150910  
 Thu Sep 10 21:45:17 2015 Z

## SOFTWARE OUTPUT

Microsoft Office File Validation Add-In v.14.0.5130.5003, 20150910  
 Thu Sep 10 21:40:41 2015 Z  
 Microsoft Visual Studio 2010 Tools for Office Runtime (x64) v.10.0.50908, 20150910  
 Thu Sep 10 21:40:31 2015 Z  
 Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219 v.10.0.40219, 20150910  
 Thu Sep 10 21:40:26 2015 Z  
 Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 v.10.0.40219, 20150910  
 Thu Sep 10 21:08:23 2015 Z  
 Microsoft Office Office 64-bit Components 2007 v.12.0.6612.1000, 20150910  
 Thu Sep 10 19:42:26 2015 Z  
 Microsoft Office OneNote MUI (English) 2007 v.12.0.6612.1000, 20150910  
 Thu Sep 10 19:26:55 2015 Z  
 Microsoft Office PowerPoint MUI (English) 2007 v.12.0.6612.1000, 20150910  
 Thu Sep 10 19:21:49 2015 Z  
 Microsoft Office Word MUI (English) 2007 v.12.0.6612.1000, 20150910  
 Thu Sep 10 19:19:37 2015 Z  
 Microsoft Office Excel MUI (English) 2007 v.12.0.6612.1000, 20150910  
 Thu Sep 10 19:16:21 2015 Z  
 Microsoft Office Proof (French) 2007 v.12.0.6612.1000, 20150910  
 Thu Sep 10 19:16:17 2015 Z  
 Microsoft Office Proof (Spanish) 2007 v.12.0.6612.1000, 20150910  
 Thu Sep 10 19:16:13 2015 Z  
 Microsoft Office Proof (English) 2007 v.12.0.6612.1000, 20150910  
 Thu Sep 10 19:12:19 2015 Z  
 Microsoft Office Shared Setup Metadata MUI (English) 2007 v.12.0.6612.1000,  
 20150910  
 Thu Sep 10 19:12:16 2015 Z  
 Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2007 v.12.0.6612.1000,  
 20150910  
 Thu Sep 10 19:12:07 2015 Z  
 Microsoft Office Shared 64-bit MUI (English) 2007 v.12.0.6612.1000, 20150910  
 Thu Sep 10 19:09:17 2015 Z  
 Microsoft Visual C++ 2005 Redistributable v.8.0.61001, 20150910  
 Thu Sep 10 18:41:27 2015 Z  
 swMSM v.12.0.0.1, 20150910  
 Thu Sep 10 16:31:32 2015 Z  
 Microsoft Office Proofing (English) 2007 v.12.0.4518.1014, 20150910  
 Fri Feb 20 17:12:44 2015 Z  
 Renesas Electronics USB 3.0 Host Controller Driver v.2.1.36.0, 20150220  
 Fri Feb 20 17:05:34 2015 Z  
 Validity Fingerprint Sensor Driver v.4.5.133.0, 20150220  
  
 S-1-5-21-3944275416-1635498007-1700510902-1000  
 Wed Sep 23 13:54:38 2015 Z  
 HPDiagnosticAlert v.1.00.0001, 20150923  
 Wed Sep 23 13:54:35 2015 Z  
 HP FWUpdateED02 v.1.2.0.0, 20150923

## SOFTWARE OUTPUT

-----  
 profilelist v.20100219

(Software) Get content of ProfileList key

Microsoft\Windows NT\CurrentVersion\ProfileList

LastWrite Time Thu Jan 7 21:15:32 2016 (UTC)

Path : %systemroot%\system32\config\systemprofile

SID : S-1-5-18

LastWrite : Tue Jul 14 04:53:25 2009 (UTC)

Path : C:\Windows\ServiceProfiles\LocalService

SID : S-1-5-19

LastWrite : Mon Dec 1 12:56:43 2014 (UTC)

Path : C:\Windows\ServiceProfiles\NetworkService

SID : S-1-5-20

LastWrite : Mon Dec 1 12:56:43 2014 (UTC)

Path : C:\Users\Abe-Arjun Malik

SID : S-1-5-21-3944275416-1635498007-1700510902-1000

LastWrite : Wed Apr 20 02:35:52 2016 (UTC)

LoadTime : Thu Jan 1 00:00:00 1970 (UTC)

Path : C:\Users\Nikita

SID : S-1-5-21-3944275416-1635498007-1700510902-1003

LastWrite : Tue Apr 19 11:25:43 2016 (UTC)

LoadTime : Thu Jan 1 00:00:00 1970 (UTC)

Domain Accounts

-----  
 regback v.20100219

(Software) List all tasks along with logfile name and last written date/time

regidle

Microsoft\Windows

NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\Registry\RegIdleBackup

LastWrite: Tue Jul 14 04:54:36 2009

Id {CA4B8FF2-A4D2-4D88-A52E-3A5BDAF7F56E}

Index 3

Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks

LastWrite Time Wed Apr 20 02:33:31 2016 (UTC)

Path : \Microsoft\Windows\Setup\gwx\refreshgwxconfig

Dynamicinfo : {016D2046-90D7-4FDE-9BBF-2A2C3EAE2CD8}

LastWrite : Sat Sep 12 13:15:09 2015 (UTC)

## SOFTWARE OUTPUT

Path : \Microsoft\Windows\SideShow\AutoWake  
 Dynamicinfo : {03FD7E44-8AFD-4244-9FE8-D41A2FB9EBF0}  
 LastWrite : Mon Dec 1 12:59:47 2014 (UTC)

Path : \Microsoft\Windows\Time Synchronization\SynchronizeTime  
 Dynamicinfo : {044A6734-E90E-4F8F-B357-B2DC8AB3B5EC}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Media Center\UpdateRecordPath  
 Dynamicinfo : {0668B03C-4366-43D2-84A5-6E3EB3E8053D}  
 LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

Path : \Microsoft\Windows\Setup\GWXTriggers\OutOfIdle-5d  
 Dynamicinfo : {074ACF14-4118-45C3-B75D-36E725095088}  
 LastWrite : Wed Apr 20 02:33:26 2016 (UTC)

Path : \OfficeSoftwareProtectionPlatform\SvcRestartTask  
 Dynamicinfo : {077D8F06-B1D9-476C-9F19-B406AF6B2CF5}  
 LastWrite : Thu Sep 10 19:43:12 2015 (UTC)

Path : \Microsoft\Windows\Tcpip\IpAddressConflict1  
 Dynamicinfo : {088482FA-65B8-4E17-9ABF-1DCD48E8D373}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Tcpip\IpAddressConflict2  
 Dynamicinfo : {09F06BFE-A3C8-40E3-846A-6E6F4000C238}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Software Updater  
 Dynamicinfo : {0A2E3A14-8F05-4884-A746-0FE15AAF46B3}  
 LastWrite : Wed Apr 20 02:35:37 2016 (UTC)

Path : \Microsoft\Windows\Setup\gwx\refreshgwxconfigandcontent  
 Dynamicinfo : {0BBCA8AC-AE39-4631-B4D9-675DC30DD6A0}  
 LastWrite : Sat Sep 12 13:15:05 2015 (UTC)

Path : \Microsoft\Windows\Media Center\MediaCenterRecoveryTask  
 Dynamicinfo : {0D13A645-EEC8-4DFF-AEE6-FEFC2F7020A5}  
 LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

Path : \Intel Security DAT Reputation (AMCore) periodic endpoint safety pulse  
 Dynamicinfo : {11B713E7-52E9-40D0-B3FA-6714546ED3C6}  
 LastWrite : Wed Apr 20 02:30:37 2016 (UTC)

Path : \Microsoft\Windows\Media Center\DispatchRecoveryTasks  
 Dynamicinfo : {1283C9FF-059A-4289-9AA3-B6108A061BC0}  
 LastWrite : Mon Dec 1 12:59:49 2014 (UTC)

## SOFTWARE OUTPUT

Path : \Microsoft\Windows\Windows Activation Technologies\ValidationTask  
 Dynamicinfo : {19C61C07-53AC-4128-B501-9717845F6123}  
 LastWrite : Fri Mar 11 01:44:20 2016 (UTC)

Path : \Microsoft\Windows\Media Center\PvrScheduleTask  
 Dynamicinfo : {1AC57DC4-7F23-4C1C-BC79-2E806661F6A3}  
 LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

Path : \Microsoft\Windows\Task Manager\Interactive  
 Dynamicinfo : {1F7B7221-AE8F-44F3-BA82-F7D260F51964}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Media Center\OCURDiscovery  
 Dynamicinfo : {218D4A56-E22D-43DA-9770-C6B5CBA08228}  
 LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

Path : \Microsoft\Windows\WindowsBackup\Windows Backup Monitor  
 Dynamicinfo : {222AE904-694A-46E1-9582-3C7DE909FA04}  
 LastWrite : Thu Feb 18 16:38:00 2016 (UTC)

Path : \Microsoft\Windows\Multimedia\SystemSoundsService  
 Dynamicinfo : {2470470F-2634-478E-B181-571E98A789BB}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Setup\gwx\refreshgwxcontent  
 Dynamicinfo : {27615632-5C66-4105-8FAC-E333E7FFDBBD}  
 LastWrite : Sat Sep 12 13:15:15 2015 (UTC)

Path : \Microsoft\Windows\Active Directory Rights Management Services  
 Client\AD RMS Rights Policy Template Management (Manual)  
 Dynamicinfo : {28011108-68DF-4C73-B91B-57427D501BBA}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\WindowsBackup\ConfigNotification  
 Dynamicinfo : {2F57269B-1E09-4E2D-AB1E-B0FDAC7D279C}  
 LastWrite : Fri Feb 19 15:00:00 2016 (UTC)

Path : \Microsoft\Windows\Media Center\ehDRMInit  
 Dynamicinfo : {3137B913-088E-4008-9B7D-BF8EC8DA6F91}  
 LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

Path : \McAfee\McAfee Idle Detection Task  
 Dynamicinfo : {32C06B88-CDE6-4B42-B422-DC0CD42872F9}  
 LastWrite : Wed Apr 20 09:07:03 2016 (UTC)

Path : \Microsoft\Windows\Media Center\ObjectStoreRecoveryTask  
 Dynamicinfo : {33ACEEDD-3731-4222-A963-07CF3DADB662}



## SOFTWARE OUTPUT

LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

Path : \Microsoft\Windows\Setup\GwxTriggers\refreshgwxconfig-B

Dynamicinfo : {3627FDB2-B57E-4960-951F-82276126E699}

LastWrite : Wed Apr 20 02:33:31 2016 (UTC)

Path : \Microsoft\Windows\SideShow\SessionAgent

Dynamicinfo : {3E7D3B64-3211-44FF-89D5-ECE1AC1E4DBB}

LastWrite : Fri Feb 20 18:43:52 2015 (UTC)

Path : \Microsoft\Windows\Media Center\mcupdate

Dynamicinfo : {3E8C4BD7-D699-4C28-9772-046CC76A26B6}

LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

Path :

\Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticResolver

Dynamicinfo : {3F851FCE-F72C-4845-89F7-C2390E1FABD8}

LastWrite : Mon Dec 1 12:59:47 2014 (UTC)

Path : \Microsoft\Windows\Windows Activation

Technologies\ValidationTaskDeadline

Dynamicinfo : {41846AC0-E3A4-4672-8898-6EC45C08E542}

LastWrite : Fri Mar 11 01:44:21 2016 (UTC)

Path : \Microsoft\Windows\Customer Experience Improvement Program\UsbCeip

Dynamicinfo : {47536D45-EEEC-4BDC-8183-A4DC1F8DA9E4}

LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Shell\WindowsParentalControlsMigration

Dynamicinfo : {486D715E-6AA2-44CF-BC48-B6990CBB53C6}

LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\TextServicesFramework\MsCtfMonitor

Dynamicinfo : {4C8B01A2-11FF-4C41-848F-508EF4F00CF7}

LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \McAfeeLogon

Dynamicinfo : {4DFBCCF3-1B77-456B-990C-1136970F8699}

LastWrite : Wed Apr 20 02:32:31 2016 (UTC)

Path : \McAfee Remediation (Prepare)

Dynamicinfo : {4FE88A5A-C255-4159-B13D-F9FB7B363BED}

LastWrite : Tue Apr 12 19:48:40 2016 (UTC)

Path : \Microsoft\Windows\Media Center\ConfigureInternetTimeService

Dynamicinfo : {50BCC072-AAE4-4ED1-83C2-C4D35C4FF9EF}

LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

## SOFTWARE OUTPUT

Path : \Microsoft\Windows\Media Center\PBDADiscoveryW2  
 Dynamicinfo : {59F1E13E-6768-4F81-9576-8D3B7FE7E2F9}  
 LastWrite : Mon Dec 1 12:59:49 2014 (UTC)

Path : \Microsoft\Windows\UPnP\UPnPHostConfig  
 Dynamicinfo : {5A40E926-9E86-4B89-9CFD-B12311724371}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Shell\WindowsParentalControls  
 Dynamicinfo : {5B42DD9C-5A26-4F27-BB95-34603F0997E5}  
 LastWrite : Fri Jan 8 02:02:17 2016 (UTC)

Path : \Microsoft\Windows\Setup\GWXTriggers\MachineUnlock-5d  
 Dynamicinfo : {5BE75BBF-95D2-4405-B4B4-B509729590E6}  
 LastWrite : Wed Apr 20 02:33:28 2016 (UTC)

Path : \Microsoft\Windows\Defrag\ScheduledDefrag  
 Dynamicinfo : {5C0AEEEE-C154-45BE-8499-BEA5F11BAFF6}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\CertificateServicesClient\SystemTask  
 Dynamicinfo : {5F5A18EB-DC73-4E45-A11C-B59043598412}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Active Directory Rights Management Services  
 Client\AD RMS Rights Policy Template Management (Automated)  
 Dynamicinfo : {613612BA-897D-44CE-8DC1-8FC283F9FD51}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Setup\GWXTriggers\OutOfSleep-5d  
 Dynamicinfo : {629B43A5-9BA6-4957-8F74-46605D6F40AB}  
 LastWrite : Wed Apr 20 02:33:28 2016 (UTC)

Path : \Microsoft\Windows\User Profile Service\HiveUploadTask  
 Dynamicinfo : {6738BA6E-EA75-4B6B-B8B8-71F0336DD8EF}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Media Center\RegisterSearch  
 Dynamicinfo : {6AB4890E-A79D-4D80-B307-C5F88F9975BC}  
 LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

Path : \Microsoft\Windows\AppID\VerifiedPublisherCertStoreCheck  
 Dynamicinfo : {72DB7465-BC54-491B-A92A-4637A28C9BBF}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Apple\AppleSoftwareUpdate  
 Dynamicinfo : {73CDEB7B-7898-4C3F-A972-3FB5E089E6D6}  
 LastWrite : Tue Apr 19 11:36:00 2016 (UTC)

## SOFTWARE OUTPUT

Path : \Microsoft\Windows\Windows Media Sharing\UpdateLibrary  
 Dynamicinfo : {753C47AE-EC5E-44B3-95A9-2C8E553F0E39}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Offline Files\Background Synchronization  
 Dynamicinfo : {7677F211-8C0B-4839-B1CA-5B67BFD6B563}  
 LastWrite : Mon Dec 1 13:00:31 2014 (UTC)

Path : \Microsoft\Windows\Setup\GWXTriggers\ScheduleUpgradeTime  
 Dynamicinfo : {76FB83A3-599D-4E65-8E1C-6EB1E6617D67}  
 LastWrite : Wed Apr 20 02:33:29 2016 (UTC)

Path : \WPD\SqmUpload\_S-1-5-21-3944275416-1635498007-1700510902-1000  
 Dynamicinfo : {78CC33BD-5DFF-47D0-B762-66DC5907DB08}  
 LastWrite : Wed Sep 23 13:44:54 2015 (UTC)

Path : \Microsoft\Windows\CertificateServicesClient\UserTask  
 Dynamicinfo : {7AFCC0CA-7121-422A-AB45-B0E8D599FF08}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Kavooceirmnou  
 Dynamicinfo : {7E3D14AC-16E1-4642-AF3B-4FFE5A571DE53}  
 LastWrite : Wed Apr 20 02:36:56 2016 (UTC)

Path : \Microsoft\Windows\NetTrace\GatherNetworkInfo  
 Dynamicinfo : {81540B9F-B5BF-47EB-9C95-BE195BF2C664}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Media Center\RecordingRestart  
 Dynamicinfo : {8279F117-2CE7-475D-8096-88A1E13F1C31}  
 LastWrite : Mon Dec 1 12:59:49 2014 (UTC)

Path : \Microsoft\Windows\MobilePC\HotStart  
 Dynamicinfo : {8348205D-8F28-4E28-9402-0DA47C86C021}  
 LastWrite : Mon Dec 1 12:59:47 2014 (UTC)

Path : \GoogleUpdateTaskMachineUA  
 Dynamicinfo : {868D64B9-2F6F-492A-AD05-A0130E46DA6D}  
 LastWrite : Wed Apr 20 02:30:37 2016 (UTC)

Path : \Microsoft\Windows\WDI\ResolutionHost  
 Dynamicinfo : {9435F817-FED2-454E-88CD-7F78FDA62C48}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\SystemRestore\SR  
 Dynamicinfo : {994C86AD-A929-4B2C-88A0-4E25A107A029}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

## SOFTWARE OUTPUT

Path : \Microsoft\Windows\CertificateServicesClient\UserTask-Roam  
 Dynamicinfo : {9979CB83-103A-4105-9E5D-C74B0AF6D198}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Media Center\SqlLiteRecoveryTask  
 Dynamicinfo : {9AAA61A9-FD89-4E88-83A2-55407FF770BB}  
 LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

Path : \Microsoft\Windows\WindowsColorSystem\Calibration Loader  
 Dynamicinfo : {A35BB7A6-5F0C-4C9F-8450-2B3BED532D51}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\AppID\PolicyConverter  
 Dynamicinfo : {A48CABBF-24C8-4B87-B00F-9261807C3B43}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Media Center\ReindexSearchRoot  
 Dynamicinfo : {A504C180-B09E-4803-B947-63290EA1966E}  
 LastWrite : Mon Dec 1 12:59:49 2014 (UTC)

Path : \Microsoft\Windows\Location\Notifications  
 Dynamicinfo : {A6AF9377-77CE-47AB-AD7D-EC32CAD0C82D}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Application Experience\AitAgent  
 Dynamicinfo : {AC4E5ACF-89F7-4220-BA21-81EE183975E2}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Ras\MobilityManager  
 Dynamicinfo : {AC668097-4D6B-4093-AC14-014C09DBF820}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\PerfTrack\BackgroundConfigSurveyor  
 Dynamicinfo : {B0CBAB43-44FC-469B-A4CE-87426761FDCE}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Setup\gwx\launchtrayprocess  
 Dynamicinfo : {B29D48B0-BBD3-408D-87EB-77B6F5BF91D7}  
 LastWrite : Sat Sep 12 13:15:17 2015 (UTC)

Path : \Microsoft\Windows\Application Experience\Microsoft Compatibility  
 Appraiser  
 Dynamicinfo : {BCDE879F-20BA-4130-8ECC-B2EC7CCE7231}  
 LastWrite : Wed Apr 20 09:07:04 2016 (UTC)

Path : \Microsoft\Windows\Diagnosis\Scheduled  
 Dynamicinfo : {BE669C13-8165-4536-96D0-6D6C39292AAE}

## SOFTWARE OUTPUT

LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Customer Experience Improvement  
Program\Consolidator  
Dynamicinfo : {C016366B-7126-46CA-B36B-592A3D95A60B}  
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Media Center\OCURActivate  
Dynamicinfo : {C5ED6D18-085F-40F3-B941-3F78A5F7E024}  
LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

Path : \Microsoft\Windows\Wininet\CacheTask  
Dynamicinfo : {C7A88055-B200-4840-A6C2-AAEA7B707A2D}  
LastWrite : Mon Dec 1 14:14:00 2014 (UTC)

Path : \Microsoft\Windows\Registry\RegIdleBackup  
Dynamicinfo : {CA4B8FF2-A4D2-4D88-A52E-3A5BDAF7F56E}  
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\RemoteAssistance\RemoteAssistanceTask  
Dynamicinfo : {CB3D64BF-C0C9-45FF-BFB0-FF1A8F680186}  
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\MemoryDiagnostic\CorruptionDetector  
Dynamicinfo : {CEE64558-E1A7-4D9D-80A7-2001912BE5B5}  
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Windows Error Reporting\QueueReporting  
Dynamicinfo : {D0250F3F-6480-484F-B719-42F659AC64D5}  
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Media Center\PBDADiscovery  
Dynamicinfo : {D410BF39-B404-419D-B896-0AD70841EE20}  
LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

Path : \Microsoft\Windows\Autochk\Proxy  
Dynamicinfo : {D7B6E81D-3CF4-432C-84D2-24213F4316E6}  
LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Maintenance\WinSAT  
Dynamicinfo : {DA41DE71-8431-42FB-9DB0-EB64A961DEAD}  
LastWrite : Fri Sep 11 21:16:54 2015 (UTC)

Path : \Microsoft\Windows\Application Experience\ProgramDataUpdater  
Dynamicinfo : {DB6BCECB-FCC6-4BDD-A8A3-5D2676E5A948}  
LastWrite : Tue Oct 20 00:50:58 2015 (UTC)

Path : \Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTask

## SOFTWARE OUTPUT

Dynamicinfo : {DD9F510C-95F4-499A-90C8-BAC5BC372FF4}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\Media Center\PBDADiscoveryW1  
 Dynamicinfo : {E1080EB3-C55A-44B5-A4F3-FE03A35310FA}  
 LastWrite : Mon Dec 1 12:59:49 2014 (UTC)

Path : \Microsoft\Windows\SideShow\SystemDataProviders  
 Dynamicinfo : {E17AD8E2-F3E1-42FA-ADA9-017DD7EED536}  
 LastWrite : Fri Feb 20 18:44:07 2015 (UTC)

Path : \Microsoft\Windows\Windows Filtering  
 Platform\BfeOnServiceStartTypeChange  
 Dynamicinfo : {E22A8667-F75B-4BA9-BA46-067ED4429DE8}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\WindowsBackup\AutomaticBackup  
 Dynamicinfo : {E262D9FE-E5A9-475D-A241-816480F6A867}  
 LastWrite : Sun Apr 17 23:00:02 2016 (UTC)

Path : \Microsoft\Windows\Bluetooth\UninstallDeviceTask  
 Dynamicinfo : {E3163C33-301D-4730-A266-5518C5ED3967}  
 LastWrite : Sun Nov 21 03:39:16 2010 (UTC)

Path :  
 \Microsoft\Windows\DiskDiagnostic\Microsoft-Windows-DiskDiagnosticDataCollector  
 Dynamicinfo : {E5490D35-2E93-460E-B9C3-0DD6FF26D902}  
 LastWrite : Sun Sep 27 09:01:56 2015 (UTC)

Path : \GoogleUpdateTaskMachineCore  
 Dynamicinfo : {E78A582D-6F8B-4AA2-A64F-EFDF503DDFF1}  
 LastWrite : Wed Apr 20 02:31:30 2016 (UTC)

Path : \Microsoft\Windows\Media Center\PeriodicScanRetry  
 Dynamicinfo : {E7A4A570-145D-40C4-837D-EE5706260AC3}  
 LastWrite : Mon Dec 1 12:59:47 2014 (UTC)

Path : \Microsoft\Windows\Media Center\PvrRecoveryTask  
 Dynamicinfo : {E7C5352E-94D5-4A42-ABFD-D5E571B602AB}  
 LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

Path : \Microsoft\Windows\Setup\GwxTriggers\ScheduleUpgradeReminderTime  
 Dynamicinfo : {E9FFE219-59B2-481A-B43E-BFDEBE492BD9}  
 LastWrite : Wed Apr 20 02:33:30 2016 (UTC)

Path : \Microsoft\Windows\Media Center\InstallPlayReady  
 Dynamicinfo : {EAAAC9511-9C44-434C-9296-047786BE455F}  
 LastWrite : Mon Dec 1 12:59:48 2014 (UTC)

## SOFTWARE OUTPUT

Path : \Microsoft\Windows\RAC\RacTask  
 Dynamicinfo : {EACA24FF-236C-401D-A1E7-B3D5267B8A50}  
 LastWrite : Sun Nov 21 03:39:16 2010 (UTC)

Path : \Microsoft\Windows\MUI\LPRemove  
 Dynamicinfo : {EB02381F-D652-4B1C-894A-712498C62C51}  
 LastWrite : Sun Nov 21 03:39:15 2010 (UTC)

Path : \Microsoft\Windows\SideShow\GadgetManager  
 Dynamicinfo : {ED80B881-78AA-402F-B596-D91BE78738A9}  
 LastWrite : Mon Dec 1 12:59:47 2014 (UTC)

Path : \{3EF99D69-2964-426C-A73E-0B7DE1D052B2}  
 Dynamicinfo : {F40BAA20-C329-4609-BE86-D3F23D8DCFC4}  
 LastWrite : Sat Feb 20 02:05:13 2016 (UTC)

Path : \Microsoft\Windows\Setup\GWXTriggers\OnIdle-5d  
 Dynamicinfo : {F6923E36-0DD6-4976-B081-66AA933DFFE9}  
 LastWrite : Wed Apr 20 03:03:26 2016 (UTC)

Path : \Microsoft\Windows\Offline Files\Logon Synchronization  
 Dynamicinfo : {F6CFB2EF-9468-4EF7-8492-27400097DB7D}  
 LastWrite : Mon Dec 1 12:59:46 2014 (UTC)

Path : \Microsoft\Windows\MemoryDiagnostic\DecompressionFailureDetector  
 Dynamicinfo : {FA2BC0A6-8D4B-458A-85C8-2B8C72487513}  
 LastWrite : Sun Nov 21 03:39:16 2010 (UTC)

Path : \Microsoft\Windows\Media Center\ActivateWindowsSearch  
 Dynamicinfo : {FAFC9076-B783-4FA5-9928-27DC976E991C}  
 LastWrite : Mon Dec 1 12:59:49 2014 (UTC)

Path : \Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem  
 Dynamicinfo : {FB3C354D-297A-4EB2-9B58-090F6361906B}  
 LastWrite : Sun Nov 21 03:39:16 2010 (UTC)

Path : \Microsoft\Windows\Setup\GWXTriggers\Logon-5d  
 Dynamicinfo : {FB78B292-273E-4567-9C00-D9539941F0A4}  
 LastWrite : Wed Apr 20 02:33:27 2016 (UTC)

Path : \Microsoft\Windows\Setup\GWXTriggers\Time-5d  
 Dynamicinfo : {FBFECABA-59EC-4AC6-A271-F720742CCF5D}  
 LastWrite : Wed Apr 20 02:33:29 2016 (UTC)

Path : \Microsoft\Windows\Customer Experience Improvement  
 Program\KernelCeipTask  
 Dynamicinfo : {FDD56C73-F0D5-41B6-B767-6EFFD7966428}

## SOFTWARE OUTPUT

LastWrite : Sun Nov 21 03:39:16 2010 (UTC)

-----  
removdev v.200800611

(Software) Parses Windows Portable Devices key (Vista)

RemovDev

Microsoft\Windows Portable Devices\Devices

LastWrite Time Wed Apr 6 14:25:07 2016 (UTC)

Device :  
LastWrite : Thu Sep 24 18:59:56 2015 (UTC)  
SN :  
Drive : Apple iPhone

Device :  
LastWrite : Sat Sep 12 00:09:28 2015 (UTC)  
SN :  
Drive : nüvi 2555

Device : DISK&VEN\_JMCR&PROD\_SD&REV\_  
LastWrite : Wed Sep 23 03:08:50 2015 (UTC)  
SN : 5&12E35340&0&000000  
Drive : F:\

Device : DISK&VEN\_&PROD\_&REV\_2.20  
LastWrite : Sat Mar 19 22:24:05 2016 (UTC)  
SN : 0718011120035AF&0  
Drive : E:\

Device : DISK&VEN\_&PROD\_&REV\_PMAP  
LastWrite : Mon Sep 14 18:42:14 2015 (UTC)  
SN : 07032B5A180AA664&0  
Drive : THUMBDRIVE

Device : DISK&VEN\_&PROD\_&REV\_PMAP  
LastWrite : Thu Oct 1 23:47:49 2015 (UTC)  
SN : 070B43D2DE271C28&0  
Drive : USB DISK

Device : DISK&VEN\_&PROD\_&REV\_PMAP  
LastWrite : Sat Mar 19 22:25:27 2016 (UTC)  
SN : 070B43D9AB6E9253&0  
Drive : USB DISK

Device : DISK&VEN\_APPLE&PROD\_IPOD&REV\_2.70  
LastWrite : Fri Nov 20 01:57:30 2015 (UTC)  
SN : 000A27001CA9A995&0



## SOFTWARE OUTPUT

Drive : ABE-ARJUN M

Device : DISK&VEN\_HP&PROD\_USB\_FLASH\_DRIVE&REV\_1.00

LastWrite : Sat Sep 12 04:20:28 2015 (UTC)

SN : 002354D46B97AC5102CF01C0&0

Drive : ITUNES

Device : DISK&VEN\_PNY&PROD\_USB\_2.0\_FD&REV\_1100

LastWrite : Fri Nov 20 01:57:20 2015 (UTC)

SN : ACB3HD1000000240&0

Drive : PHOTOS

Device : DISK&VEN\_PNY&PROD\_USB\_2.0\_FD&REV\_8192

LastWrite : Mon Oct 19 13:06:32 2015 (UTC)

SN : AABA1ECC00001167&0

Drive : USB20FD

Device : DISK&VEN\_SANDISK&PROD\_CRUZER&REV\_1.20

LastWrite : Mon Oct 26 09:56:12 2015 (UTC)

SN : 200544568018E7B0762E&0

Drive : F:\

Device : DISK&VEN\_SANDISK&PROD\_CRUZER&REV\_8.02

LastWrite : Fri Feb 20 17:01:44 2015 (UTC)

SN : 17380302D5A10198&0

Drive : F:\

Device : DISK&VEN\_SANDISK&PROD\_CRUZER\_MICRO&REV\_8.02

LastWrite : Wed Apr 6 14:25:07 2016 (UTC)

SN : 2243400CB8E0533D&0

Drive : F:\

Device : DISK&VEN\_SONY&PROD\_DSC&REV\_1.00

LastWrite : Fri Nov 20 01:55:59 2015 (UTC)

SN : C68B200FB019&0

Drive : G:\

Device : DISK&VEN\_SONY&PROD\_DSC&REV\_1.00

LastWrite : Fri Nov 20 01:56:02 2015 (UTC)

SN : C68B200FB019&1

Drive : H:\

Device : DISK&VEN\_SONY&PROD\_DSC&REV\_1.00

LastWrite : Fri Nov 20 01:55:58 2015 (UTC)

SN : C68B200FB019&2

Drive : PMHOME

-----

## SOFTWARE OUTPUT

renocide v.20130425

(Software) Check for Renocide malware

Microsoft\DRM\amty not found.

-----  
schedagent v.20100817

(Software) Get SchedulingAgent key contents

Microsoft\SchedulingAgent

LastWrite Time Tue Jul 14 05:08:49 2009 (UTC)

OldName = 37L4247E29-32

LogPath = %SystemRoot%\Tasks\SCHEDLGU.TXT

MaxLogSizeKB = 32

TasksFolder = %SystemRoot%\Tasks

-----  
secctr v.20100310

(Software) Get data from Security Center key

secctr

Microsoft\Security Center

LastWrite Time Wed Apr 20 02:39:31 2016 (UTC)

cval 0x01

-----  
sfc v.20100305

(Software) Get SFC values

sfc v.20100305

Microsoft\Windows NT\CurrentVersion\Winlogon

LastWrite Time Wed Apr 20 02:36:52 2016 (UTC)

Policies\Microsoft\Windows NT\Windows File Protection

LastWrite Time Tue Jul 14 04:49:20 2009 (UTC)

-----  
shellexec v.20130410

(Software) Gets ShellExecuteHooks from Software hive

Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks

LastWrite Time Tue Jul 14 04:53:25 2009 (UTC)

Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks has no values. No  
ShellExecuteHooks installed.

## SOFTWARE OUTPUT

Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks  
 LastWrite Time Tue Jul 14 04:53:25 2009 (UTC)

Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks has no  
 values. No ShellExecuteHooks installed.

-----  
 shellex v.20100515

(Software) Gets Shell Extensions from Software hive

Microsoft\Windows\CurrentVersion\Shell Extensions\Approved  
 LastWrite Time Thu Jan 7 22:15:26 2016 (UTC)

{C41662BB-1FA0-4CE0-8DC5-9B7F8279FF97} Microsoft Office Thumbnail Handler  
 DLL: C:\Program Files\Common Files\Microsoft Shared\OFFICE14\msoshext.dll  
 Timestamp: Thu Sep 10 19:54:03 2015 Z

{00C6D95F-329C-409a-81D7-C46C66EA7F33}  
 DLL: %SystemRoot%\System32\shdocvw.dll  
 Timestamp: Tue Apr 12 08:28:59 2011 Z

{80009818-f38f-4af1-87b5-eadaab9433e58} MF ADTS Property Handler  
 DLL: %SystemRoot%\System32\mf.dll  
 Timestamp: Tue Jul 14 04:53:38 2009 Z

{42042206-2D85-11D3-8CFF-005004838597} Microsoft Office HTML Icon Handler  
 DLL: C:\Program Files\Microsoft Office\Office14\MSOHEVI.DLL  
 Timestamp: Thu Sep 10 16:32:34 2015 Z

{B41DB860-64E4-11D2-9906-E49FADC173CA} WinRAR shell extension  
 DLL: C:\Program Files\WinRAR\rarext.dll  
 Timestamp: Thu Sep 10 19:07:29 2015 Z

{ABBE31D0-6DAE-11D0-BECA-00C04FD940BE} Subscription Mgr  
 DLL: C:\Windows\System32\webcheck.dll  
 Timestamp: Mon Dec 1 14:13:54 2014 Z

{D66DC78C-4F61-447F-942B-3FB6980118CF} {D66DC78C-4F61-447F-942B-3FB6980118CF}  
 DLL: C:\Program Files\Microsoft Office\Office14\VISSHE.DLL  
 Timestamp: Thu Sep 10 19:54:05 2015 Z

{F5175861-2688-11d0-9C5E-00AA00A45957} Subscription Folder  
 DLL: C:\Windows\System32\webcheck.dll  
 Timestamp: Mon Dec 1 14:13:54 2014 Z

{993BE281-6695-4BA5-8A2A-7AACBFAAB69E} Microsoft Office Metadata Handler  
 DLL: C:\Program Files\Common Files\Microsoft Shared\OFFICE14\msoshext.dll  
 Timestamp: Thu Sep 10 19:54:03 2015 Z

## SOFTWARE OUTPUT

```

{08165EA0-E946-11CF-9C87-00AA005127ED} WebCheckWebCrawler
  DLL: C:\Windows\System32\webcheck.dll
  Timestamp: Mon Dec 1 14:13:54 2014 Z

{506F4668-F13E-4AA1-BB04-B43203AB3CC0} {506F4668-F13E-4AA1-BB04-B43203AB3CC0}
  DLL: C:\Program Files\Microsoft Office\Office14\VISSHE.DLL
  Timestamp: Thu Sep 10 19:54:05 2015 Z

{7D559C10-9FE9-11d0-93F7-00AA0059CE02} Code Download Agent
  DLL: C:\Windows\System32\webcheck.dll
  Timestamp: Mon Dec 1 14:13:54 2014 Z

{B41DB860-8EE4-11D2-9906-E49FADC173CA} WinRAR shell extension
  DLL:
  Timestamp: Thu Jan 1 00:00:00 1970 Z

{0006F045-0000-0000-C000-000000000046} Microsoft Outlook Custom Icon Handler
  DLL: C:\Program Files\Microsoft Office\Office14\OLKFSTUB.DLL
  Timestamp: Thu Sep 10 21:28:35 2015 Z

{E6FB5E20-DE35-11CF-9C87-00AA005127ED} WebCheck
  DLL:
  Timestamp: Thu Jan 1 00:00:00 1970 Z

{B9E1D2CB-CCFF-4AA6-9579-D7A4754030EF} iTunes
  DLL: C:\Program Files\iTunes\iTunesMiniPlayer.dll
  Timestamp: Thu Jan 7 22:15:26 2016 Z

{7FC0B86E-5FA7-11d1-BC7C-00C04FD929DB} WebCheck SyncMgr Handler
  DLL: C:\Windows\System32\webcheck.dll
  Timestamp: Mon Dec 1 14:13:54 2014 Z

{7CCA70DB-DE7A-4FB7-9B2B-52E2335A3B5A} Nameext
  DLL: C:\Program Files\Microsoft Office\Office14\NAMEEXT.DLL
  Timestamp: Thu Sep 10 21:28:35 2015 Z

```

-----  
shelloverlay v.20100308

(Software) Gets ShellIconOverlayIdentifiers values

shelloverlay

Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers  
LastWrite Time Tue Apr 12 08:28:45 2011 (UTC)

Tue Apr 12 08:28:45 2011 Z

Offline Files {4E77131D-3629-431c-9818-C5679DC83E81}

Tue Jul 14 04:53:25 2009 Z

## SOFTWARE OUTPUT

EnhancedStorageShell {D9144DCD-E998-4ECA-AB6A-DCD83CCBA16D}  
 SharingPrivate {08244EE6-92F0-47f2-9FC9-929BAA2E7235}

-----  
 snapshot v.20080725

(Software) Check ActiveX comp kill bit; Access Snapshot

ActiveX Snapshot Vuln  
 Microsoft\Internet Explorer

IE Version = 9.11.9600.18282

GUID: {F0E42D50-368C-11D0-AD81-00A0C90DC8D9}  
 Compatibility Flags 0x400

GUID: {F0E42D60-368C-11D0-AD81-00A0C90DC8D9}  
 Compatibility Flags 0x400

GUID: {F2175210-368C-11D0-AD81-00A0C90DC8D9}  
 Compatibility Flags 0x400

-----  
 soft\_run v.20130603

(Software) [Autostart] Get autostart key contents from Software hive

Microsoft\Windows\CurrentVersion\Run  
 LastWrite Time Thu Jan 7 22:15:24 2016 (UTC)  
 iTunesHelper - "C:\Program Files\iTunes\iTunesHelper.exe"

Microsoft\Windows\CurrentVersion\Run has no subkeys.

Microsoft\Windows\CurrentVersion\RunOnce  
 LastWrite Time Thu Feb 18 16:23:07 2016 (UTC)  
 Microsoft\Windows\CurrentVersion\RunOnce has no values.  
 Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.

Microsoft\Windows\CurrentVersion\RunServices not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\Run  
 LastWrite Time Tue Feb 2 00:33:07 2016 (UTC)  
 NUSB3MON - "C:\Program Files (x86)\Renesas Electronics\USB 3.0 Host Controller  
 Driver\Application\nusb3mon.exe"  
 IndexSearch - "C:\Program Files (x86)\Nuance\PaperPort\IndexSearch.exe"  
 Nuance PDF Create 8-reminder - "C:\Program Files (x86)\Nuance\PDF Create  
 8\Ereg\Ereg.exe" -r "C:\ProgramData\Nuance\PDF Create 8\Ereg\Ereg.ini"  
 PaperPort PTD - "C:\Program Files (x86)\Nuance\PaperPort\pptd40nt.exe"  
 QuickTime Task - "C:\Program Files (x86)\QuickTime\QTTask.exe" -atboottime  
 BCSSync - "C:\Program Files (x86)\Microsoft Office\Office14\BCSSync.exe"

## SOFTWARE OUTPUT

/DelayServices

PDFHook - C:\Program Files (x86)\Nuance\PDF Viewer Plus\pdfpro5hook.exe

HP Software Update - C:\Program Files (x86)\Hp\HP Software Update\HPWuSchd2.exe

PDF5 Registry Controller - C:\Program Files (x86)\Nuance\PDF Viewer

Plus\RegistryController.exe

ControlCenter4 - C:\Program Files (x86)\ControlCenter4\BrCcBoot.exe /autorun

BrStsMon00 - C:\Program Files (x86)\Browny02\Brother\BrStMonW.exe /AUTORUN

Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no subkeys.

Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce

LastWrite Time Sun Feb 21 01:16:12 2016 (UTC)

Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no values.

Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.

Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run not found.

Microsoft\Windows NT\CurrentVersion\Terminal

Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.

Microsoft\Windows NT\CurrentVersion\Terminal

Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.

-----  
spp\_clients v.20130429

(Software) Determines volumes monitored by VSS

SPP\_Clients

Microsoft\Windows NT\CurrentVersion\SPP\Clients

LastWrite Time Thu Feb 18 16:38:09 2016 (UTC)

Monitored volumes: \\?\Volume{2c8d8b44-b930-11e4-820a-806e6f6e6963}\:HP Elitebook  
(C%3A)-----  
sql\_lastconnect v.20090112

(Software) MDAC cache of successful connections

Microsoft\MSSQLServer\Client\SuperSocketNetLib\LastConnect

MDAC Cache of successful connections

LastWrite Time Fri Feb 20 18:42:16 2015 (UTC)

BVTSQL1 84672521:tcp:BVTSQL1,1433

-----  
ssid v.20100301

(Software) Get WZCSVC SSID Info

## SOFTWARE OUTPUT

Microsoft\WZCSVC\Parameters\Interfaces not found.  
 Microsoft\EAPOL\Parameters\Interfaces not found.

-----  
 startmenuinternetapps\_lm v.20101219  
 (SOFTWARE) Start Menu Internet Applications info

## Start Menu Internet Applications

[Thu Sep 10 21:30:14 2015 (UTC)] Calendar  
 VALUE: (default) -> Microsoft Outlook  
 SUBKEY: [Thu Sep 10 21:32:12 2015 (UTC)] Microsoft Outlook

[Thu Sep 10 21:30:14 2015 (UTC)] Contacts  
 VALUE: (default) -> Microsoft Outlook  
 SUBKEY: [Tue Jul 14 04:55:00 2009 (UTC)] Address Book  
 SUBKEY: [Thu Sep 10 21:32:12 2015 (UTC)] Microsoft Outlook

[Thu Sep 10 16:33:31 2015 (UTC)] EnvelopeHost  
 VALUE: no values.  
 SUBKEY: [Thu Sep 10 16:33:30 2015 (UTC)] Microsoft Excel  
 SUBKEY: [Thu Sep 10 16:33:31 2015 (UTC)] Microsoft Word

[Thu Sep 10 21:32:12 2015 (UTC)] Mail  
 VALUE: (default) -> Microsoft Outlook  
 SUBKEY: [Thu Sep 10 21:32:12 2015 (UTC)] Microsoft Outlook  
 SUBKEY: [Tue Jul 14 04:55:00 2009 (UTC)] Windows Mail

[Thu Jan 7 22:15:24 2016 (UTC)] Media  
 VALUE: no values.  
 SUBKEY: [Thu Jan 7 22:15:24 2016 (UTC)] iTunes  
 SUBKEY: [Thu Jan 7 22:07:26 2016 (UTC)] QuickTime  
 SUBKEY: [Tue Apr 12 08:28:45 2011 (UTC)] Windows Media Center  
 SUBKEY: [Tue Jul 14 04:55:00 2009 (UTC)] Windows Media Player

[Fri Jan 1 20:52:18 2016 (UTC)] StartMenuInternet  
 VALUE: (default) -> IEXPLORE.EXE  
 SUBKEY: [Fri Jan 1 20:52:18 2016 (UTC)] FIREFOX.EXE  
 SUBKEY: [Fri Sep 11 14:57:00 2015 (UTC)] Google Chrome  
 SUBKEY: [Mon Dec 1 14:13:22 2014 (UTC)] IEXPLORE.EXE

-----  
 svchost v.20100322  
 (Software) Get entries from SvcHost key

## SOFTWARE OUTPUT

svchost

Microsoft\Windows NT\CurrentVersion\SvcHost  
 LastWrite Time Wed Apr 13 11:40:56 2016 (UTC)

RPCSS                RpcEptMapper,RpcSs  
 defragsvc          defragsvc  
 LocalSystemNetworkRestricted  
 UxSms,WdiSystemHost,Netman,trkwks,AudioEndpointBuilder,WUDFSvc,IPBusEnum,hidserv,dot  
 3svc,irmon,sysmain,PcaSvc,homegrouplistener,WPDBusEnum,wlansvc,TabletInputService,Cs  
 cService,UmRdpService,StorSvc  
 LocalService  
 nsi,WdiServiceHost,w32time,EventSystem,RemoteRegistry,WinHttpAutoProxySvc,sppuinotif  
 y,THREADORDER,netprofm,lltdsvc,fdphost,SstpSvc,WebClient,FontCache  
 netsvcs  
 AeLookupSvc,CertPropSvc,SCPolicySvc,lanmanserver,gpsvc,IKEEXT,AudioSrv,FastUserSwitc  
 hingCompatibility,Ias,Irmon,Nla,Ntmssvc,NWWorkstation,Nwsapagent,Rasauto,Rasman,Rem  
 oteaccess,SENS,Sharedaccess,SRSservice,Tapisrv,Wmi,WmdmPmSp,TermService,wuauserv,BITS  
 ,ShellHWDetection,LogonHours,PCAudit,helpsvc,uploadmgr,iphlpssvc,seclogon,AppInfo,msi  
 scsi,MMCSS,winmgmt,SessionEnv,browser,EapHost,schedule,hkmsvc,wercplsupport,ProfSvc,  
 Themes,BDESVC,AppMgmt  
 WerSvcGroup        wersvc  
 LocalServiceNoNetwork DPS,PLA,BFE,mpssvc,WwanSvc  
 termsvcs           TermService  
 swprv              swprv  
 LocalServiceNetworkRestricted  
 DHCP,eventlog,AudioSrv,BthHFSrv,LmHosts,wscsvc,homegroupprovider,WPCSvc  
 LocalServicePeerNet PNRPSvc,p2pimsvc,p2psvc,PnrpAutoReg  
 NetworkServiceAndNoImpersonation KtmRm

regsvc              RemoteRegistry  
 LocalServiceAndNoImpersonation  
 SSDPSRV,upnphost,SCardSvr,fdrespub,AppIDSvc,QWAVE,wcncsvc,SensrSvc,Mcx2Svc  
 DcomLaunch        Power,PlugPlay,DcomLaunch  
 NetworkServiceNetworkRestricted PolicyAgent

NetworkService  
 CryptSvc,DHCP,TermService,DNSCache,lanmanworkstation,NapAgent,nlasvc,WinRM,WECSVC,Ta  
 pirsrv  
 sdrsvc              sdrsvc  
 WbioSvcGroup       WbioSrv  
 imgsrv              StiSvc  
 wcssvc              WcsPlugInService  
 AxInstSVGroup      AxInstSV  
 secsvcs            WinDefend  
 bthsvcs            bthserv



## SOFTWARE OUTPUT

PeerDist            PeerDistSvc  
GPSvcGroup        GPSvc  
utcsvc            DiagTrack

-----  
Launching tracing v.20120509

Microsoft\Tracing

Fri Feb 20 18:42:16 2015	Explorer_RASAPI32
Fri Feb 20 18:42:16 2015	Explorer_RASMANCS
Fri Feb 20 18:42:16 2015	IENRCORE_RASAPI32
Fri Feb 20 18:42:16 2015	IENRCORE_RASMANCS
Wed Feb 10 01:31:19 2016	InstallHMAVPN_RASAPI32
Wed Feb 10 01:31:19 2016	InstallHMAVPN_RASMANCS
Tue Jul 14 05:08:52 2009	IpHlpSvc
Wed Nov 11 20:32:01 2015	IPNATHLP
Fri Sep 11 15:49:41 2015	KMDDSP
Thu Sep 10 17:10:00 2015	McCBEntAndInstru_RASAPI32
Thu Sep 10 17:13:04 2015	mcinfo_RASAPI32
Wed Nov 11 22:07:48 2015	mcinfo_RASMANCS
Thu Sep 10 17:10:00 2015	McPartnerSAInstallManager_RASAPI32
Thu Sep 10 20:09:36 2015	McPltCmd_RASAPI32
Wed Nov 11 20:36:15 2015	McPltCmd_RASMANCS
Thu Sep 10 20:11:25 2015	McSmtFwk_RASAPI32
Wed Nov 11 20:36:18 2015	McSmtFwk_RASMANCS
Thu Feb 25 02:06:15 2016	McSvHost_RASAPI32
Thu Sep 10 17:10:00 2015	mcsync_RASAPI32
Thu Feb 11 12:57:01 2016	McSync_RASMANCS
Thu Sep 10 17:11:59 2015	mcuicnt_RASAPI32
Thu Sep 10 17:10:00 2015	mcupdate_RASAPI32
Thu Sep 10 17:12:03 2015	MCUPDA~1_RASAPI32
Wed Nov 11 22:06:20 2015	MCUPDA~1_RASMANCS
Thu Sep 10 17:13:30 2015	mcupdutl_RASAPI32
Wed Nov 11 22:08:05 2015	mcupdutl_RASMANCS
Fri Sep 11 15:50:02 2015	NDPTSP
Wed Nov 11 20:32:00 2015	PPP
Wed Nov 11 20:32:00 2015	RASCCP
Wed Nov 11 20:32:00 2015	RASEAP
Wed Nov 11 20:32:01 2015	RASIPCP
Wed Nov 11 20:32:01 2015	RASIPHLP
Wed Nov 11 20:32:01 2015	RASIPV6CP
Wed Nov 11 20:31:56 2015	RASMAN
Wed Nov 11 20:32:00 2015	RASPAP
Tue Jul 14 05:01:47 2009	RASPLAP
Wed Nov 11 20:31:56 2015	RASTAPI
Sat Feb 20 01:50:51 2016	SoftwareUpdater_RASAPI32
Sat Feb 20 01:50:52 2016	SoftwareUpdater_RASMANCS
Wed Nov 11 20:32:02 2015	svchost_RASAPI32
Wed Nov 11 20:32:00 2015	svchost_RASCHAP
Tue Jul 14 05:09:58 2009	svchost_RASDLG

## SOFTWARE OUTPUT

```

Wed Nov 11 20:32:02 2015  svchost_RASMANCS
Wed Nov 11 20:31:56 2015  tapi32
Fri Sep 11 15:48:49 2015  tapisrv
Wed Nov 11 20:32:01 2015  VPNIKE

Wow6432Node\Microsoft\Tracing
Sun Nov 29 23:55:23 2015  agent_RASAPI32
Fri Sep 11 15:51:57 2015  CLVIEW_RASAPI32
Sat Sep 12 00:21:11 2015  express_RASAPI32
Sat Sep 12 00:21:11 2015  express_RASMANCS
Sat Feb 20 02:08:19 2016  FreeYouTubeDownloadManager_RASAPI32
Sat Feb 20 02:08:19 2016  FreeYouTubeDownloadManager_RASMANCS
Sat Sep 12 00:18:01 2015  GarminService_RASAPI32
Sat Sep 12 00:18:01 2015  GarminService_RASMANCS
Wed Feb 10 01:36:32 2016  HMA! Pro VPN_RASAPI32
Wed Feb 10 01:36:32 2016  HMA! Pro VPN_RASMANCS
Thu Sep 10 16:45:01 2015  Install_RASAPI32
Tue Jan 19 22:21:34 2016  IntuitUpdater_RASAPI32
Tue Jan 19 22:21:34 2016  IntuitUpdater_RASMANCS
Tue Jan 19 22:20:32 2016  IntuitUpdateService_RASAPI32
Tue Jan 19 22:20:32 2016  IntuitUpdateService_RASMANCS
Thu Sep 10 16:40:56 2015  KSLDJiaKk_RASAPI32
Thu Sep 10 16:40:56 2015  KSLDJiaKk_RASMANCS
Thu Sep 10 16:46:02 2015  kusimeem_RASAPI32
Thu Sep 10 16:46:02 2015  kusimeem_RASMANCS
Thu Sep 10 16:45:09 2015  McItInfo_RASAPI32
Thu Sep 10 23:02:39 2015  OUTLOOK_RASAPI32
Tue Sep 29 01:24:02 2015  rundll32_RASAPI32
Sat Feb 20 01:50:02 2016  rundll32_RASMANCS
Fri Sep 11 15:48:49 2015  tapi32
Tue Jan 19 22:40:02 2016  TurboTax_RASAPI32
Tue Jan 19 22:40:02 2016  TurboTax_RASMANCS
Thu Sep 10 16:38:23 2015  WebCompanionInstaller_RASAPI32
Thu Sep 10 16:38:23 2015  WebCompanionInstaller_RASMANCS
Thu Sep 10 16:39:18 2015  WebCompanion_RASAPI32
Thu Sep 10 16:39:18 2015  WebCompanion_RASMANCS

```

-----  
uninstall v.20140512

(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT  
hives

Uninstall

Microsoft\Windows\CurrentVersion\Uninstall

Thu Mar 10 13:44:09 2016 (UTC)

Microsoft .NET Framework 4.5.2 v.4.5.51209

## SOFTWARE OUTPUT

Thu Mar 10 13:37:50 2016 (UTC)

Microsoft Office Office 64-bit Components 2010 v.14.0.7015.1000

Thu Feb 4 20:02:22 2016 (UTC)

Microsoft Visual C++ 2005 Redistributable (x64) v.8.0.61000

Tue Feb 2 00:22:42 2016 (UTC)

PaperPort Image Printer 64-bit v.14.00.0000

Tue Feb 2 00:14:47 2016 (UTC)

Microsoft Visual C++ 2005 Redistributable (x64) v.8.0.59192

Thu Jan 14 16:38:03 2016 (UTC)

Microsoft Silverlight v.5.1.41212.0

Thu Jan 7 22:40:42 2016 (UTC)

iTunes v.12.3.2.35

Thu Jan 7 22:11:08 2016 (UTC)

Bonjour v.3.1.0.1

Thu Jan 7 22:10:49 2016 (UTC)

Apple Mobile Device Support v.9.1.0.6

Thu Jan 7 22:10:10 2016 (UTC)

Apple Application Support (64-bit) v.4.1.2

Mon Dec 21 11:42:17 2015 (UTC)

Microsoft .NET Framework 4.5.2 v.4.5.51209

Mon Sep 21 00:23:57 2015 (UTC)

PDF-Viewer v.2.5.315.0

Fri Sep 11 15:59:21 2015 (UTC)

Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2010 v.14.0.7015.1000

Fri Sep 11 15:59:19 2015 (UTC)

Microsoft Office Shared 64-bit MUI (English) 2010 v.14.0.7015.1000

Thu Sep 10 21:40:41 2015 (UTC)

Microsoft Visual Studio 2010 Tools for Office Runtime (x64) v.10.0.50903

Microsoft Visual Studio 2010 Tools for Office Runtime (x64) v.10.0.50908

Thu Sep 10 21:40:31 2015 (UTC)

Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219 v.10.0.40219

Thu Sep 10 21:08:23 2015 (UTC)

Microsoft Office Office 64-bit Components 2007 v.12.0.6612.1000

## SOFTWARE OUTPUT

Thu Sep 10 19:12:16 2015 (UTC)

Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2007 v.12.0.6612.1000

Thu Sep 10 19:12:07 2015 (UTC)

Microsoft Office Shared 64-bit MUI (English) 2007 v.12.0.6612.1000

Thu Sep 10 19:07:29 2015 (UTC)

WinRAR 5.01 (64-bit) v.5.01.0

Fri Feb 20 18:42:16 2015 (UTC)

DXM\_Runtime

MPlayer2

Fri Feb 20 17:05:34 2015 (UTC)

Validity Fingerprint Sensor Driver v.4.5.133.0

Tue Jul 14 04:53:26 2009 (UTC)

AddressBook

Connection Manager

DirectDrawEx

Fontcore

IE40

IE4Data

IE5BAKEX

IEData

MobileOptionPack

SchedulingAgent

WIC

Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

Tue Apr 19 01:22:35 2016 (UTC)

McAfee Total Protection v.14.0.7086

Mon Apr 18 01:10:07 2016 (UTC)

Mozilla Maintenance Service v.45.0.2.5941

Mon Apr 18 01:10:05 2016 (UTC)

Mozilla Firefox 45.0.2 (x86 en-US) v.45.0.2

Wed Apr 13 19:24:10 2016 (UTC)

McAfee WebAdvisor v.4.0.187

Wed Apr 13 11:38:25 2016 (UTC)

Security Update for Microsoft Office 2010 (KB2956063) 32-Bit Edition

Update for Microsoft Office 2010 (KB2589318) 32-Bit Edition

Security Update for Microsoft Office 2010 (KB2881071) 32-Bit Edition

## SOFTWARE OUTPUT

Update for Microsoft Office 2010 (KB2589375) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB3114989) 32-Bit Edition  
 Security Update for Microsoft Office 2010 (KB2881029) 32-Bit Edition  
 Security Update for Microsoft Office 2010 (KB2553313) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB2794737) 32-Bit Edition  
 Security Update for Microsoft Office 2010 (KB2880971) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB3085512) 32-Bit Edition  
 Security Update for Microsoft Office 2010 (KB2850016) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB2553140) 32-Bit Edition  
 Security Update for Microsoft Office 2010 (KB3085528) 32-Bit Edition  
 Security Update for Microsoft Outlook 2010 (KB3114883) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB3054873) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB2597087) 32-Bit Edition  
 Update for Microsoft Filter Pack 2.0 (KB2999508) 32-Bit Edition  
 Security Update for Microsoft Word 2010 (KB3114993) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB3054886) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB2553388) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB3055047) 32-Bit Edition  
 Update for Microsoft Outlook 2010 (KB2760779) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB2883019) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB2589298) 32-Bit Edition  
 Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition  
 Update for Microsoft Outlook Social Connector 2010 (KB2553308) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB3114555) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB2589352) 32-Bit Edition  
 Update for Microsoft Office 2010 (KB3114750) 32-Bit Edition  
 Definition Update for Microsoft Office 2010 (KB3114999) 32-Bit Edition

Wed Apr 13 11:38:24 2016 (UTC)

Microsoft Office Outlook 2010 v.14.0.7015.1000

Wed Apr 13 11:37:14 2016 (UTC)

Update for Microsoft Office 2007 suites (KB2596787) 32-Bit Edition  
 Security Update for Microsoft Office 2007 suites (KB2881067) 32-Bit Edition  
 Security Update for Microsoft Office PowerPoint 2007 (KB2596912) 32-Bit Edition  
 Security Update for Microsoft Office OneNote 2007 (KB2889915) 32-Bit Edition  
 Security Update for Microsoft Office 2007 suites (KB2596871) 32-Bit Edition  
 Security Update for Microsoft Office Word 2007 (KB3114983) 32-Bit Edition  
 Security Update for Microsoft Office 2007 suites (KB2597969) 32-Bit Edition  
 Security Update for Microsoft Office Compatibility Pack Service Pack 3 (KB3114982)  
 32-Bit Edition  
 Security Update for Microsoft Office 2007 suites (KB2760591) 32-Bit Edition  
 Security Update for Microsoft Office 2007 suites (KB3114742) 32-Bit Edition  
 Security Update for Microsoft Office 2007 suites (KB2880507) 32-Bit Edition  
 Security Update for Microsoft Office 2007 suites (KB2956110) 32-Bit Edition  
 Security Update for Microsoft Office 2007 suites (KB2880508) 32-Bit Edition  
 Security Update for Microsoft Office 2007 suites (KB2850022) 32-Bit Edition

## SOFTWARE OUTPUT

Microsoft Office 2007 Service Pack 3 (SP3)

Update for Microsoft Office 2007 suites (KB2965286) 32-Bit Edition

Security Update for Microsoft Office 2007 suites (KB2760585) 32-Bit Edition

Security Update for Microsoft Office 2007 suites (KB3085549) 32-Bit Edition

Security Update for Microsoft Office InfoPath 2007 (KB2687440) 32-Bit Edition

Update for Microsoft Office 2007 suites (KB2596620) 32-Bit Edition

Security Update for Microsoft Office 2007 suites (KB2687409) 32-Bit Edition

Security Update for Microsoft Office Compatibility Pack Service Pack 3 (KB3114895)

32-Bit Edition

Security Update for Microsoft Office 2007 suites (KB2596754) 32-Bit Edition

Security Update for Microsoft Office 2007 suites (KB2596825) 32-Bit Edition

Security Update for Microsoft Office PowerPoint 2007 (KB3114429) 32-Bit Edition

Security Update for Microsoft Office 2007 suites (KB2825645) 32-Bit Edition

Update for 2007 Microsoft Office System (KB967642)

Security Update for Microsoft Office Excel 2007 (KB3114892) 32-Bit Edition

Security Update for Microsoft Office 2007 suites (KB2596650) 32-Bit Edition

Security Update for Microsoft Office 2007 suites (KB2596792) 32-Bit Edition

Update for Microsoft Office 2007 suites (KB2767916) 32-Bit Edition

Security Update for Microsoft Office 2007 suites (KB3114542) 32-Bit Edition

Security Update for Microsoft Office 2007 suites (KB2881069) 32-Bit Edition

Wed Apr 13 11:37:12 2016 (UTC)

Microsoft Office Home and Student 2007 v.12.0.6612.1000

Fri Apr 8 11:35:26 2016 (UTC)

1Click DVD Copy 6.1.0.6

Sun Mar 27 20:36:19 2016 (UTC)

DVD43 Plug-in v1.0.0.6

Sun Mar 27 20:34:05 2016 (UTC)

1Click DVD Copy Pro 5.1.0.6

Sun Mar 27 02:09:38 2016 (UTC)

Vimtag v2.12.2.1512241007 v.v2.12.2.1512241007

Thu Mar 10 13:44:04 2016 (UTC)

Security Update for Microsoft .NET Framework 4.5.2 (KB3135996) v.1

Thu Mar 10 13:37:50 2016 (UTC)

Update for Microsoft OneNote 2010 (KB3114410) 32-Bit Edition

Security Update for Microsoft Office 2010 (KB2553313) 32-Bit Edition

Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition

Update for Microsoft Filter Pack 2.0 (KB2999508) 32-Bit Edition

Update for Microsoft Office 2010 (KB3054886) 32-Bit Edition

Security Update for Microsoft InfoPath 2010 (KB3114414) 32-Bit Edition

Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Update for Microsoft Office 2010 (KB2589352) 32-Bit Edition

## SOFTWARE OUTPUT

Update for Microsoft SharePoint Workspace 2010 (KB2760601) 32-Bit Edition

Sat Feb 20 02:05:23 2016 (UTC)

vanBasco's Karaoke Player

Sat Feb 20 01:50:11 2016 (UTC)

Videograbber v.1.0.0.0

Sat Feb 20 01:50:09 2016 (UTC)

Videograbber v.1.0.0.0

Fri Feb 19 22:20:57 2016 (UTC)

Google Chrome v.48.0.2564.116

Tue Feb 16 01:28:08 2016 (UTC)

Adobe Flash Player 20 NPAPI v.20.0.0.306

Tue Feb 9 22:20:38 2016 (UTC)

Microsoft Office Outlook MUI (English) 2010 v.14.0.7015.1000

Security Update for Microsoft Word 2010 (KB2965313) 32-Bit Edition

Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition

Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Update for Microsoft Outlook 2010 (KB3114756) 32-Bit Edition

Tue Feb 9 22:18:37 2016 (UTC)

Security Update for Microsoft .NET Framework 4.5.2 (KB3122656) v.1

Tue Feb 9 22:07:41 2016 (UTC)

Security Update for Microsoft .NET Framework 4.5.2 (KB3127229) v.1

Sat Feb 6 19:50:38 2016 (UTC)

TurboTax 2015 WinPerFedFormset v.015.000.1781

Sat Feb 6 19:50:27 2016 (UTC)

TurboTax 2015 wmdiper v.015.000.1163

Thu Feb 4 20:01:56 2016 (UTC)

MSXML 4.0 SP3 Parser (KB2758694) v.4.30.2117.0

Thu Feb 4 14:19:10 2016 (UTC)

Google Update Helper v.1.3.29.5

Tue Feb 2 00:31:58 2016 (UTC)

Brother MFL-Pro Suite MFC-9340CDW v.1.0.1.0

Tue Feb 2 00:21:29 2016 (UTC)

Nuance PDF Viewer Plus v.5.30.3290

## SOFTWARE OUTPUT

Tue Feb 2 00:21:28 2016 (UTC)  
Scansoft PDF Professional

Tue Feb 2 00:19:36 2016 (UTC)  
Nuance PaperPort 12 v.12.1.0005

Tue Feb 2 00:11:50 2016 (UTC)  
Microsoft Visual C++ 2005 Redistributable v.8.0.59193

Tue Feb 2 00:09:45 2016 (UTC)  
MSXML 4.0 SP3 Parser v.4.30.2100.0

Tue Jan 19 22:39:08 2016 (UTC)  
TurboTax 2015 WinPerFuegoContent v.015.000.0355

Tue Jan 19 22:36:17 2016 (UTC)  
TurboTax 2015 WinPerTaxSupport v.015.000.0175

Tue Jan 19 22:34:36 2016 (UTC)  
TurboTax 2015 WinPerReleaseEngine v.015.000.0423

Tue Jan 19 22:20:19 2016 (UTC)  
TurboTax 2015 v.2015.0

Tue Jan 19 22:16:20 2016 (UTC)  
TurboTax 2015 wrapper v.015.000.0126

Wed Jan 13 23:15:11 2016 (UTC)  
Google Earth v.7.1.5.1557

Tue Jan 12 01:31:02 2016 (UTC)  
Audiograbber MP3 Plugin v.1.0

Tue Jan 12 01:30:29 2016 (UTC)  
Audiograbber 1.83 Pro v.1.83 SE

Thu Jan 7 22:10:30 2016 (UTC)  
Apple Software Update v.2.1.4.131

Thu Jan 7 22:09:15 2016 (UTC)  
Apple Application Support (32-bit) v.4.1.2

Thu Jan 7 22:07:26 2016 (UTC)  
QuickTime 7 v.7.78.80.95

Wed Nov 11 22:05:10 2015 (UTC)  
Microsoft Office Shared MUI (English) 2010 v.14.0.7015.1000  
Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition



## SOFTWARE OUTPUT

Update for Microsoft Office 2010 (KB2553140) 32-Bit Edition  
 Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition  
 Security Update for Microsoft Office 2010 (KB2956076) 32-Bit Edition  
 Security Update for Microsoft Office 2010 (KB3085560) 32-Bit Edition

Wed Nov 11 22:04:39 2015 (UTC)  
 Update for Microsoft Office 2007 suites (KB2596787) 32-Bit Edition  
 Microsoft Office 2007 Service Pack 3 (SP3)  
 Update for Microsoft Office 2007 Help for Common Features (KB963673)  
 Update for Microsoft Office Script Editor Help (KB963671)  
 Security Update for Microsoft Office 2007 suites (KB3085620) 32-Bit Edition

Wed Nov 11 22:04:38 2015 (UTC)  
 Microsoft Office Shared MUI (English) 2007 v.12.0.6612.1000

Mon Oct 19 23:08:06 2015 (UTC)  
 Microsoft Outlook 2010 v.14.0.7015.1000

Tue Oct 13 22:43:12 2015 (UTC)  
 Malwarebytes Anti-Malware version 2.2.0.1024 v.2.2.0.1024

Wed Sep 23 14:00:34 2015 (UTC)  
 HP HD Webcam [Fixed] v.3.5.8.2

Wed Sep 23 13:54:38 2015 (UTC)  
 HPDiagnosticAlert v.1.00.0001

Wed Sep 23 13:54:35 2015 (UTC)  
 HP FWUpdateED02 v.1.2.0.0

Wed Sep 16 04:30:09 2015 (UTC)  
 HP Update v.5.005.002.002

Fri Sep 11 15:59:34 2015 (UTC)  
 Microsoft Office Proofing (English) 2010 v.14.0.7015.1000

Fri Sep 11 15:59:32 2015 (UTC)  
 Microsoft Office Proof (English) 2010 v.14.0.7015.1000

Fri Sep 11 15:59:28 2015 (UTC)  
 Microsoft Office Proof (French) 2010 v.14.0.7015.1000

Fri Sep 11 15:59:24 2015 (UTC)  
 Microsoft Office Proof (Spanish) 2010 v.14.0.7015.1000

Fri Sep 11 15:59:11 2015 (UTC)  
 Microsoft Office Shared Setup Metadata MUI (English) 2010 v.14.0.7015.1000

## SOFTWARE OUTPUT

Thu Sep 10 23:33:01 2015 (UTC)

Microsoft Office Outlook Connector v.14.0.6123.5001

Thu Sep 10 22:17:48 2015 (UTC)

Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition

Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Update for Microsoft Office 2010 (KB3055042) 32-Bit Edition

Thu Sep 10 22:17:45 2015 (UTC)

Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition

Update for Microsoft Office 2010 (KB3055042) 32-Bit Edition

Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Thu Sep 10 22:17:42 2015 (UTC)

Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Update for Microsoft Office 2010 (KB3055042) 32-Bit Edition

Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition

Thu Sep 10 21:45:17 2015 (UTC)

Microsoft Office File Validation Add-In v.14.0.5130.5003

Thu Sep 10 21:45:04 2015 (UTC)

Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition

Thu Sep 10 21:45:01 2015 (UTC)

Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition

Thu Sep 10 21:44:48 2015 (UTC)

Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition

Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Thu Sep 10 21:42:53 2015 (UTC)

Update for Microsoft Office 2010 (KB2553347) 32-Bit Edition

Service Pack 2 for Microsoft Office 2010 (KB2687455) 32-Bit Edition

Thu Sep 10 21:40:31 2015 (UTC)

{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757

{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2467173

{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860

{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655

{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743

{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063

{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573

Thu Sep 10 21:40:26 2015 (UTC)

Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 v.10.0.40219

## SOFTWARE OUTPUT

{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757  
 {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173  
 {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860  
 {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655  
 {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743  
 {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063  
 {F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573

Thu Sep 10 21:08:23 2015 (UTC)

Microsoft Office 2007 Service Pack 3 (SP3)

Security Update for Microsoft Office 2007 suites (KB2825645) 32-Bit Edition

Thu Sep 10 19:42:26 2015 (UTC)

Microsoft Office OneNote MUI (English) 2007 v.12.0.6612.1000

Update for Microsoft Office OneNote 2007 Help (KB963670)

Microsoft Office 2007 Service Pack 3 (SP3)

Thu Sep 10 19:26:55 2015 (UTC)

Microsoft Office PowerPoint MUI (English) 2007 v.12.0.6612.1000

Update for Microsoft Office Powerpoint 2007 Help (KB963669)

Microsoft Office 2007 Service Pack 3 (SP3)

Thu Sep 10 19:21:49 2015 (UTC)

Microsoft Office Word MUI (English) 2007 v.12.0.6612.1000

Update for Microsoft Office Word 2007 Help (KB963665)

Microsoft Office 2007 Service Pack 3 (SP3)

Thu Sep 10 19:19:37 2015 (UTC)

Microsoft Office Excel MUI (English) 2007 v.12.0.6612.1000

Update for Microsoft Office Excel 2007 Help (KB963678)

Microsoft Office 2007 Service Pack 3 (SP3)

Thu Sep 10 19:16:21 2015 (UTC)

Microsoft Office Proof (French) 2007 v.12.0.6612.1000

Microsoft Office Proofing Tools 2007 Service Pack 3 (SP3)

Thu Sep 10 19:16:17 2015 (UTC)

Microsoft Office Proof (Spanish) 2007 v.12.0.6612.1000

Microsoft Office Proofing Tools 2007 Service Pack 3 (SP3)

Thu Sep 10 19:16:13 2015 (UTC)

Microsoft Office Proof (English) 2007 v.12.0.6612.1000

Microsoft Office Proofing Tools 2007 Service Pack 3 (SP3)

Thu Sep 10 19:13:39 2015 (UTC)

Microsoft Office Home and Student 2007 v.12.0.6612.1000

Thu Sep 10 19:12:19 2015 (UTC)

## SOFTWARE OUTPUT

Microsoft Office Shared Setup Metadata MUI (English) 2007 v.12.0.6612.1000  
 Microsoft Office 2007 Service Pack 3 (SP3)

Thu Sep 10 19:12:16 2015 (UTC)  
 Microsoft Office 2007 Service Pack 3 (SP3)

Thu Sep 10 19:12:07 2015 (UTC)  
 Microsoft Office 2007 Service Pack 3 (SP3)

Thu Sep 10 19:09:17 2015 (UTC)  
 Microsoft Visual C++ 2005 Redistributable v.8.0.61001

Thu Sep 10 18:41:27 2015 (UTC)  
 swMSM v.12.0.0.1

Thu Sep 10 16:31:32 2015 (UTC)  
 Microsoft Office Proofing (English) 2007 v.12.0.4518.1014

Thu Sep 10 16:27:07 2015 (UTC)  
 Adobe Photoshop Elements 2.0 v.2.0

Thu Sep 10 16:19:56 2015 (UTC)  
 Hoyle Puzzle and Board Games 2011 (remove only)

Fri Feb 20 18:42:16 2015 (UTC)  
 InstallShield Uninstall Information  
 Renesas Electronics USB 3.0 Host Controller Driver v.2.1.36.0

Fri Feb 20 17:12:44 2015 (UTC)  
 Renesas Electronics USB 3.0 Host Controller Driver v.2.1.36.0

Tue Jul 14 04:53:25 2009 (UTC)  
 AddressBook  
 Connection Manager  
 DirectDrawEx  
 Fontcore  
 IE40  
 IE4Data  
 IE5BAKEX  
 IEData  
 MobileOptionPack  
 SchedulingAgent  
 WIC

-----  
 urlzone v.20090526  
 (Software) URLZONE detection

## SOFTWARE OUTPUT

Microsoft\Windows\CurrentVersion\Internet Settings\urlzone not found.  
 Microsoft\Windows NT\CurrentVersion\Image File Execution Options\userinit.exe not found.

-----  
 uac v.20130213

(Software) Get Select User Account Control (UAC) Values from  
 HKLMSOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

## UAC Information

Microsoft\Windows\CurrentVersion\policies\system  
 LastWrite Time Sun Dec 13 17:44:46 2015 (UTC)

EnableLUA value = 1

User Account Control: Run all administrators in Admin Approval Mode

0 = Disabled

1 = Enabled (Default)

EnableVirtualization value = 1

User Account Control: Virtualize file and registry write failures to per-user locations

0 = Disabled

1 = Enabled (Default)

FilterAdministratorToken value = 0

User Account Control: Admin Approval Mode for the built-in Administrator account

0 = Disabled (Default)

1 = Enabled

ConsentPromptBehaviorAdmin value = 5

User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode

0 = Elevate without prompting

1 = Prompt for credentials on the secure desktop

2 = Prompt for consent on the secure desktop

3 = Prompt for credentials

4 = Prompt for consent

5 = Prompt for consent for non-Windows binaries (Default)

ConsentPromptBehaviorUser value = 3

User Account Control: Behavior of the elevation prompt for standard users

0 = Automatically deny elevation requests

1 = Prompt for consent on the secure desktop

3 = Prompt for consent on the secure desktop (Default)

## SOFTWARE OUTPUT

-----  
 virut v.20130425  
 (Software) Detect Virut artifacts

Microsoft\Windows\CurrentVersion\Explorer  
 LastWrite Time Mon Sep 21 00:23:58 2015 (UTC)

UpdateHost value not found.

Also be sure to check the SYSTEM\ControlSet00n\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\AuthorizedApplications\List key for exceptions added to the firewall; use the fw\_config.pl plugin.

-----  
 win\_cv v.20090312  
 (Software) Get & display the contents of the Windows\CurrentVersion key

Microsoft\Windows\CurrentVersion  
 LastWrite Time Wed Sep 16 13:38:09 2015 (UTC)

SM\_GamesName : Games  
 ProgramFilesPath : %ProgramFiles%  
 DevicePath : %SystemRoot%\inf  
 ProgramFilesDir : C:\Program Files  
 ProgramW6432Dir : C:\Program Files  
 MediaPathUnexpanded : %SystemRoot%\Media  
 ProgramFilesDir (x86) : C:\Program Files (x86)  
 CommonFilesDir : C:\Program Files\Common Files  
 CommonW6432Dir : C:\Program Files\Common Files  
 SM\_ConfigureProgramsName : Set Program Access and Defaults  
 CommonFilesDir (x86) : C:\Program Files (x86)\Common Files

-----  
 winbackup v.20120812  
 (Software) Get Windows Backup

Microsoft\Windows\CurrentVersion\WindowsBackup\ScheduleParams\TargetDevice  
 LastWrite Time Thu Feb 18 20:29:59 2016 (UTC)

PresentableName = G:\  
 UniqueName = \\?\Volume{c0e9ffaf-960c-11e5-ac0f-402cf486a5d9}\  
 Label = FreeAgent Drive  
 DeviceVendor = Seagate  
 DeviceProduct = FreeAgent  
 DeviceVersion = 0132  
 DeviceSerial = 2GEYC3F8

Microsoft\Windows\CurrentVersion\WindowsBackup\Status  
 LastWrite Time Sun Apr 17 23:00:02 2016 (UTC)

## SOFTWARE OUTPUT

LastResultTime = Sun Apr 17 23:00:02 2016 (UTC)  
 LastResultTarget = \\?\Volume{c0e9ffaf-960c-11e5-ac0f-402cf486a5d9}\  
 LastResultTargetPresentableName = G:\  
 LastResultTargetLabel = FreeAgent Drive

-----  
 winlogon v.20130425

(Software) Get values from the WinLogon key

Microsoft\Windows NT\CurrentVersion\Winlogon

LastWrite Time Wed Apr 20 02:36:52 2016 (UTC)

LegalNoticeCaption =

LegalNoticeText =

ReportBootOk = 1

AutoRestartShell = 1

ForceUnlockLogon = 0

PasswordExpiryWarning = 5

PowerdownAfterShutdown = 0

ShutdownWithoutLogon = 0

WinStationsDisabled = 0

DisableCAD = 1

scremoveoption = 0

AutoAdminLogon = 0

CachedLogonsCount = 10

DebugServerCommand = no

ShutdownFlags = 39

Background = 0 0 0

Shell = explorer.exe

DefaultUserName = Abe-Arjun Malik

Userinit = C:\Windows\system32\userinit.exe,

PreCreateKnownFolders = {A520A1A4-1780-4FF6-BD18-167343C5AF16}

VMApplet = SystemPropertiesPerformance.exe /pagefile

Notify subkey contents:

igfxcui - Fri Feb 20 18:22:43 2015

DLLName: igfxdev.dll

Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon

LastWrite Time Sat Sep 12 03:43:52 2015 (UTC)

DefaultDomainName =

DefaultUserName =

ReportBootOk = 1

Shell = explorer.exe

Userinit = userinit.exe,

PreCreateKnownFolders = {A520A1A4-1780-4FF6-BD18-167343C5AF16}

VMApplet = SystemPropertiesPerformance.exe /pagefile

## SOFTWARE OUTPUT

Notify subkey not found.

Analysis Tips: The UserInit and Shell values are executed when a user logs on. The UserInit value should contain a reference to userinit.exe; the Shell value should contain just 'explorer.exe'. Check TaskMan & System values, if found.

Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList not found.

-----  
winnt\_cv v.20080609

(Software) Get & display the contents of the Windows NT\CurrentVersion key

WinNT\_CV

Microsoft\Windows NT\CurrentVersion

LastWrite Time Wed Apr 13 11:42:16 2016 (UTC)

RegisteredOrganization :

CurrentVersion : 6.1

CurrentBuild : 7601

CurrentBuildNumber : 7601

CSDBuildNumber : 1130

SoftwareType : System

InstallationType : Client

SystemRoot : C:\Windows

PathName : C:\Windows

EditionID : Professional

CSDVersion : Service Pack 1

RegisteredOwner : Abe-Arjun Malik

CurrentType : Multiprocessor Free

ProductName : Windows 7 Professional

ProductId : 00371-OEM-9083366-15357

BuildLab : 7601.win7sp1\_ldr.160317-0600

InstallDate : Thu Sep 10 04:09:09 2015 (UTC)

BuildGUID : 28e17687-ccfd-496c-b560-327ba0ce8baa

BuildLabEx : 7601.23392.amd64fre.win7sp1\_ldr.160317-0600

DigitalProductId : a4 00 00 00 03 00 00 00 30 30 33 37 31 2d 4f 45 4d 2d 39 30 38  
33 33 36 36 2d 31 35 33 35 37 00 b4 00 00 00 58 31 35 2d 33 37 33 36 39 00 00 00 00  
00 00 00 ba ec 51 90 2b 9e 0b 03 6c ce e5 b1 4c 2b 03 00 00 00 00 00 47 56 f1 55 0b  
19 dd ce 02 00  
00  
00 36  
d2 79 58

DigitalProductId4 : f8 04 00 00 04 00 00 00 30 00 30 00 33 00 37 00 31 00 2d 00 30  
00 30 00 31 00 38 00 30 00 2d 00 38 00 33 00 33 00 2d 00 36 00 31 00 35 00 33 00 35  
00 37 00 2d 00 30 00 32 00 2d 00 31 00 30 00 33 00 33 00 2d 00 37 00 36 00 30 00 31  
00 2e 00 30 00 30 00 30 00 30 00 2d 00 32 00 35 00 33 00 32 00 30 00 31 00 35 00 00  
00  
00 00 00 65 00 31 00 32 00 30 00 65 00 38 00 36 00 38 00 2d 00 33 00 64 00 66 00 32  
00 2d 00 34 00 36 00 34 00 61 00 2d 00 39 00 35 00 61 00 30 00 2d 00 62 00 35 00 32



## SOFTWARE OUTPUT

[illegible]

winver v.20081210

```
(Software) Get Windows version
```

```
ProductName = Windows 7 Professional
```

CSDVersion = Service Pack 1

```
InstallDate = Thu Sep 10 04:09:09 2015
```

yahoo\_lm v.20101219

## SOFTWARE OUTPUT

(SOFTWARE) Yahoo Messenger parser

Yahoo not found.

-----  
ALERT: appinitdlls: Entry not blank: C:\WINDOWS\system32\nvinitx.dll  
ALERT: appinitdlls: Entry not blank: C:\WINDOWS\SysWOW64\nvinit.dll  
ALERT: cmd\_shell: Clients\StartMenuInternet\IExplore.exe\shell\open\command warning:  
C:\Program Files\Internet Explorer\iexplore.exe  
WARNING: winlogon: Microsoft\Windows NT\CurrentVersion\Winlogon GinaDLL value found:  
pssogina.dll  
Alert: svc: AdobeFlashPlayerUpdateSvc has a WOW64 value: 1  
Alert: svc: atashost has a WOW64 value: 1  
Alert: svc: clr\_optimization\_v2.0.50727\_32 has a WOW64 value: 1  
Alert: svc: CVPNDRVA has a WOW64 value: 1  
Alert: svc: gupdate has a WOW64 value: 1  
Alert: svc: gupdatem has a WOW64 value: 1  
Alert: svc: MozillaMaintenance has a WOW64 value: 1  
Alert: svc: PerfHost has a WOW64 value: 1  
Alert: svc: WIMMount has a WOW64 value: 1  
ALERT: svcdll: wbem found in path: Winmgmt -> %SystemRoot%\system32\wbem\WMIsvc.dll  
ALERT: svcdll: Relative path detected: WinHttpAutoProxySvc -> winhttp.dll  
ALERT: cmd\_shell: Clients\StartMenuInternet\IExplore.exe\shell\open\command warning:  
C:\Program Files\Internet Explorer\iexplore.exe

## SECURITY OUTPUT

auditpol v.20121128

(Security) Get audit policy from the Security hive file

auditpol

Policy\PolAdtEv

LastWrite Time Thu Jan 7 21:08:51 2016 (UTC)

Length of data: 138 bytes.

```

0x00000000: 00 01 00 00 09 00 00 00 78 00 00 00 01 00 00 00 .....X.....
0x00000010: 03 00 00 00 03 00 03 00 01 00 01 00 00 00 01 00 .....
0x00000020: 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 .....
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 .....
0x00000050: 01 00 00 00 00 00 00 00 00 00 01 00 00 00 03 00 .....
0x00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000070: 00 00 00 00 00 00 00 00 05 00 09 00 0c 00 03 00 .....
0x00000080: 04 00 06 00 06 00 04 00 04 00 .....

```

\*\*Auditing is NOT enabled.

lsasecrets v.20140408

(Security) TEST - Get update times for LSA Secrets

Domain secret - \$MACHINE.ACC

\$MACHINE.ACC key not found

polacdms v.20100531

(Security) Get local machine SID from Security hive

PolAcDmS

Policy\PolAcDmS

LastWrite Time Fri Feb 20 18:42:15 2015 (UTC)

Machine SID: S-1-5-21-3944275416-1635498007-1700510902

PolPrDmS

Policy\PolPrDmS

LastWrite Time Tue Jul 14 04:45:54 2009 (UTC)

Primary Domain SID: S-1-5-

ALERT: appinitdls: Entry not blank: C:\WINDOWS\system32\nvinitx.dll

ALERT: appinitdls: Entry not blank: C:\WINDOWS\SysWOW64\nvinit.dll

ALERT: cmd\_shell: Clients\StartMenuInternet\IExplore.exe\shell\open\command warning:  
C:\Program Files\Internet Explorer\iexplore.exeWARNING: winlogon: Microsoft\Windows NT\CurrentVersion\Winlogon GinaDLL value found:  
pssogina.dll

Alert: svc: AdobeFlashPlayerUpdateSvc has a WOW64 value: 1

Alert: svc: atashost has a WOW64 value: 1

SECURITY OUTPUT

Alert: svc: clr\_optimization\_v2.0.50727\_32 has a WOW64 value: 1  
Alert: svc: CVPNDRVA has a WOW64 value: 1  
Alert: svc: gupdate has a WOW64 value: 1  
Alert: svc: gupdatem has a WOW64 value: 1  
Alert: svc: MozillaMaintenance has a WOW64 value: 1  
Alert: svc: PerfHost has a WOW64 value: 1  
Alert: svc: WIMMount has a WOW64 value: 1  
ALERT: svcdll: wbem found in path: Winmgmt -> %SystemRoot%\system32\wbem\WMISvc.dll  
ALERT: svcdll: Relative path detected: WinHttpAutoProxySvc -> winhttp.dll

## SAM OUTPUT

samparse v.20120722

(SAM) Parse SAM file for user &amp; group mbrshp info

## User Information

```

-----
Username       : Administrator [500]
Full Name      :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Thu Sep 10 17:03:39 2015 Z
Last Login Date : Thu Sep  3 17:49:14 2015 Z
Pwd Reset Date  : Sun Nov 21 03:57:24 2010 Z
Pwd Fail Date   : Never
Login Count     : 17
--> Password does not expire
--> Account Disabled
--> Normal user account

```

```

Username       : Guest [501]
Full Name      :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    : Default Guest Acct
Account Created : Thu Sep 10 17:03:39 2015 Z
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
--> Password does not expire
--> Account Disabled
--> Password not required
--> Normal user account

```

```

Username       : Abe-Arjun Malik [1000]
Full Name      :
User Comment    :
Account Type    : Default Admin User
Account Created : Thu Sep 10 04:09:02 2015 Z
Password Hint   : Modem
Last Login Date : Wed Apr 20 02:31:21 2016 Z
Pwd Reset Date  : Sun Mar 20 23:49:20 2016 Z
Pwd Fail Date   : Wed Apr 20 02:31:26 2016 Z
Login Count     : 365
--> Password does not expire
--> Password not required
--> Normal user account

```

```

Username       : HomeGroupUser$ [1002]

```

## SAM OUTPUT

Full Name : HomeGroupUser\$  
 User Comment : Built-in account for homegroup access to the computer  
 Account Type : Custom Limited Acct  
 Account Created : Thu Sep 10 04:09:04 2015 Z  
 Last Login Date : Never  
 Pwd Reset Date : Thu Sep 10 04:09:04 2015 Z  
 Pwd Fail Date : Fri Jan 8 02:01:55 2016 Z  
 Login Count : 0  
 --> Password does not expire  
 --> Normal user account

Username : Nikita [1003]  
 Full Name : Nikita  
 User Comment :  
 Account Type : Custom Limited Acct  
 Account Created : Thu Jan 7 21:08:09 2016 Z  
 Last Login Date : Tue Apr 19 10:59:45 2016 Z  
 Pwd Reset Date : Never  
 Pwd Fail Date : Never  
 Login Count : 169  
 --> Password does not expire  
 --> Normal user account

-----  
 Group Membership Information  
 -----

Group Name : Users [3]  
 LastWrite : Thu Jan 7 21:08:10 2016 Z  
 Group Comment : Users are prevented from making accidental or intentional  
 system-wide changes and can run most applications  
 Users :  
     S-1-5-4  
     S-1-5-21-3944275416-1635498007-1700510902-1003  
     S-1-5-11

Group Name : Event Log Readers [0]  
 LastWrite : Tue Jul 14 04:45:47 2009 Z  
 Group Comment : Members of this group can read event logs from local machine  
 Users : None

Group Name : Guests [1]  
 LastWrite : Fri Feb 20 18:42:15 2015 Z  
 Group Comment : Guests have the same access as members of the Users group by  
 default, except for the Guest account which is further restricted  
 Users :  
     S-1-5-21-3944275416-1635498007-1700510902-501

Group Name : Distributed COM Users [0]

## SAM OUTPUT

LastWrite : Tue Jul 14 04:45:47 2009 Z  
 Group Comment : Members are allowed to launch, activate and use Distributed COM objects on this machine.  
 Users : None

Group Name : Administrators [2]  
 LastWrite : Thu Sep 10 04:09:03 2015 Z  
 Group Comment : Administrators have complete and unrestricted access to the computer/domain  
 Users :  
     S-1-5-21-3944275416-1635498007-1700510902-500  
     S-1-5-21-3944275416-1635498007-1700510902-1000

Group Name : Network Configuration Operators [0]  
 LastWrite : Mon Dec 1 12:58:38 2014 Z  
 Group Comment : Members in this group can have some administrative privileges to manage configuration of networking features  
 Users : None

Group Name : Cryptographic Operators [0]  
 LastWrite : Mon Dec 1 12:58:38 2014 Z  
 Group Comment : Members are authorized to perform cryptographic operations.  
 Users : None

Group Name : Power Users [0]  
 LastWrite : Mon Dec 1 12:58:38 2014 Z  
 Group Comment : Power Users are included for backwards compatibility and possess limited administrative powers  
 Users : None

Group Name : Performance Log Users [0]  
 LastWrite : Tue Jul 14 04:45:46 2009 Z  
 Group Comment : Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer  
 Users : None

Group Name : Replicator [0]  
 LastWrite : Mon Dec 1 12:58:38 2014 Z  
 Group Comment : Supports file replication in a domain  
 Users : None

Group Name : Performance Monitor Users [0]  
 LastWrite : Tue Jul 14 04:45:46 2009 Z  
 Group Comment : Members of this group can access performance counter data locally and remotely  
 Users : None

## SAM OUTPUT

Group Name : Remote Desktop Users [0]  
 LastWrite : Mon Dec 1 12:58:38 2014 Z  
 Group Comment : Members in this group are granted the right to logon remotely  
 Users : None

Group Name : IIS\_IUSRS [1]  
 LastWrite : Tue Jul 14 04:45:47 2009 Z  
 Group Comment : Built-in group used by Internet Information Services.  
 Users :  
 S-1-5-17

Group Name : Backup Operators [0]  
 LastWrite : Mon Dec 1 12:58:38 2014 Z  
 Group Comment : Backup Operators can override security restrictions for the sole  
 purpose of backing up or restoring files  
 Users : None

## Analysis Tips:

- For well-known SIDs, see <http://support.microsoft.com/kb/243330>
- S-1-5-4 = Interactive
- S-1-5-11 = Authenticated Users
- Correlate the user SIDs to the output of the ProfileList plugin

-----  
 ALERT: appinitdls: Entry not blank: C:\WINDOWS\system32\nvinitx.dll  
 ALERT: appinitdls: Entry not blank: C:\WINDOWS\SysWOW64\nvinit.dll  
 ALERT: cmd\_shell: Clients\StartMenuInternet\IEExplore.exe\shell\open\command warning:  
 C:\Program Files\Internet Explorer\iexplore.exe  
 WARNING: winlogon: Microsoft\Windows NT\CurrentVersion\Winlogon GinaDLL value found:  
 pssogina.dll  
 Alert: svc: AdobeFlashPlayerUpdateSvc has a WOW64 value: 1  
 Alert: svc: atashost has a WOW64 value: 1  
 Alert: svc: clr\_optimization\_v2.0.50727\_32 has a WOW64 value: 1  
 Alert: svc: CVPNDRVA has a WOW64 value: 1  
 Alert: svc: gupdate has a WOW64 value: 1  
 Alert: svc: gupdatem has a WOW64 value: 1  
 Alert: svc: MozillaMaintenance has a WOW64 value: 1  
 Alert: svc: PerfHost has a WOW64 value: 1  
 Alert: svc: WIMMount has a WOW64 value: 1  
 ALERT: svcdll: wbem found in path: Winmgmt -> %SystemRoot%\system32\wbem\WMIsvc.dll  
 ALERT: svcdll: Relative path detected: WinHttpAutoProxySvc -> winhttp.dll



## SYSTEM OUTPUT

ControlSet001\Control\Session Manager\AppCertDlls not found.

-----  
appcompatcache v.20140724

(System) Parse files from System hive Shim Cache

Signature: 0xbadc0fee

Win2K8R2/Win7, 64-bit

C:\WINDOWS\SysWOW64\regsvr32.exe

ModTime: Tue Jul 14 01:14:30 2009 Z

Executed

C:\WINDOWS\splwow64.exe

ModTime: Sun Nov 21 03:24:16 2010 Z

Executed

C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe

ModTime: Tue Nov 3 01:12:02 2015 Z

Executed

C:\WINDOWS\TEMP\B6494415-6E89-4CF2-8694-AD96AB7332CE\dismhost.exe

ModTime: Fri May 30 08:07:49 2014 Z

Executed

C:\WINDOWS\system32\makecab.exe

ModTime: Tue Jul 14 01:39:16 2009 Z

Executed

C:\Program Files\HP\HP Photosmart 7520 series\Bin\InstanceFinderDlg.exe

ModTime: Wed Oct 17 08:27:47 2012 Z

Executed

C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE

ModTime: Thu Nov 19 21:11:47 2015 Z

Executed

C:\Windows\SysWOW64\net1.exe

ModTime: Sun Nov 21 03:24:16 2010 Z

Executed

C:\Program Files

(x86)\McAfee\SiteAdvisor\{3CDA9858-A1AF-4912-95A3-FFFDE8887928}\saInst.exe

ModTime: Mon Mar 28 17:31:33 2016 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\is-N87S9.tmp\mbam-setup.tmp

ModTime: Fri Mar 25 02:13:03 2016 Z

Executed

## SYSTEM OUTPUT

C:\Windows\TEMP\6223A7B9-F3CD-4170-A247-DE8306874AAB\dismhost.exe  
ModTime: Sat Nov 29 16:13:49 2014 Z  
Executed

C:\Windows\Installer\MSI4051.tmp  
ModTime: Thu Jan 14 16:37:04 2016 Z  
Executed

C:\WINDOWS\system32\{F33C3B9B-72AF-418A-B3FD-560646F7CDA2}.bat  
ModTime: Mon Apr 18 16:25:28 2016 Z

C:\WINDOWS\System32\spoolsv.exe  
ModTime: Sun Nov 21 03:24:27 2010 Z  
Executed

C:\Windows\SysWOW64\InstallShield\\_ISDEL.EXE  
ModTime: Wed Jun 10 21:48:31 2009 Z  
Executed

C:\WINDOWS\SysWOW64\windowspowershell\v1.0\powershell.exe  
ModTime: Tue Jul 14 01:39:20 2009 Z  
Executed

C:\WINDOWS\SysWOW64\tasklist.exe  
ModTime: Tue Jul 14 01:14:42 2009 Z  
Executed

C:\Program Files (x86)\Mozilla Maintenance Service\update\updater.exe  
ModTime: Fri Feb 12 15:10:26 2016 Z  
Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\nchuninst\uninst.exe  
ModTime: Fri Feb 5 14:17:26 2016 Z  
Executed

C:\WINDOWS\SysNative\dism.exe  
ModTime: Tue Jul 14 01:39:06 2009 Z

C:\Program Files (x86)\Common Files\Apple\Mobile Device  
Support\MDCrashReportTool.exe  
ModTime: Wed Oct 7 16:43:33 2015 Z  
Executed

C:\Program Files (x86)\Adobe\Photoshop Elements 2\psicon.dll  
ModTime: Mon Oct 14 18:35:09 2002 Z

C:\WINDOWS\TEMP\InstallPlugin\_20\_0\_0\_235.exe  
ModTime: Tue Dec 1 18:12:58 2015 Z

## SYSTEM OUTPUT

Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB2972106-x64.exe

ModTime: Thu Mar 10 21:02:27 2016 Z

Executed

C:\ProgramData\Dell\drivers\multiplatform\_bios\_btrfstboot\applyconfig.bat

ModTime: Fri Sep 27 05:56:57 2013 Z

C:\Windows\TEMP\CR\_5FFB2.tmp\setup.exe

ModTime: Fri Jan 15 16:59:05 2016 Z

Executed

C:\Windows\System32\diskcopy.dll

ModTime: Tue Jul 14 01:40:31 2009 Z

C:\WINDOWS\system32\reg.exe

ModTime: Tue Jul 14 01:14:30 2009 Z

Executed

c:\738a018c74a5cf8b8d5489dd\Setup.exe

ModTime: Wed May 28 11:34:26 2014 Z

Executed

C:\Program Files (x86)\HP\HP Software Update\hpwuschd2.exe

ModTime: Thu May 30 18:50:09 2013 Z

Executed

C:\Program Files

(x86)\McAfee\SiteAdvisor\{AEF1B64A-FB8F-4507-AE22-E91E60B30E39}\saInst.exe

ModTime: Tue Apr 12 15:43:08 2016 Z

Executed

C:\WINDOWS\CCM\ccmeval.exe

ModTime: Tue Apr 14 08:00:00 2015 Z

Executed

C:\WINDOWS\SysWOW64\cscript.exe

ModTime: Sat Oct 12 01:15:48 2013 Z

Executed

C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\mscorlib.exe

ModTime: Thu Mar 18 18:27:13 2010 Z

Executed

C:\Program Files (x86)\Pointsec\Pointsec for PC\P95tray.exe

ModTime: Tue Oct 8 22:56:21 2013 Z

Executed

## SYSTEM OUTPUT

C:\Program Files\Windows Mail\wab.exe

ModTime: Sun Nov 21 03:24:32 2010 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\nsr7381.tmp

ModTime: Tue Jul 7 13:30:41 2015 Z

Executed

C:\Windows\System32\vdslldr.exe

ModTime: Tue Jul 14 01:39:49 2009 Z

Executed

C:\Windows\system32\Wat\WatAdminSvc.exe

ModTime: Mon Dec 1 14:16:44 2014 Z

Executed

C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerPlugin\_20\_0\_0\_306.exe

ModTime: Tue Feb 16 01:28:08 2016 Z

Executed

C:\Windows\System32\mmcshext.dll

ModTime: Tue Jul 14 01:41:26 2009 Z

C:\WINDOWS\SoftwareDistribution\Download\Install\Silverlight\_x64.exe

ModTime: Wed Jan 13 00:22:46 2016 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\{4CB3C8EB-762B-4170-B950-54F6C845E8F1}\InstallFlashPlayer.exe

ModTime: Sat Feb 6 20:05:50 2016 Z

Executed

C:\Users\Nikita\Downloads\TXEI\_Intel\_Win7\_64\_VER1101064\SetupTXE.exe

ModTime: Wed Jan 22 07:42:11 2014 Z

C:\Windows\system32\SearchFilterHost.exe

ModTime: Sat Nov 29 16:05:18 2014 Z

Executed

C:\Windows\SysWOW64\icaccls.exe

ModTime: Tue Jul 14 01:14:21 2009 Z

Executed

C:\WINDOWS\TEMP\GLJ81EC.tmp

ModTime: Mon Apr 18 15:53:46 2016 Z

Executed

## SYSTEM OUTPUT

C:\WINDOWS\TEMP\{8DE20547-0501-4200-8194-993185C298F1}\ISBEW64.exe  
ModTime: Mon Apr 18 15:57:38 2016 Z  
Executed

C:\\_SMSTaskSequence\Packages\FDA002D5\OSD-ciscoanyconnectinstall.cmd  
ModTime: Mon Nov 17 14:22:30 2014 Z

C:\Program Files  
(x86)\McAfee\SiteAdvisor\{4CE3CA3E-4996-4920-86C7-C9FB39D679C1}\saInst.exe  
ModTime: Tue Dec 29 20:57:46 2015 Z  
Executed

C:\Users\Nikita\AppData\Local\Microsoft\Windows\Burn\Burn\SmartGesture\_Win7\_64\_VER22  
14\Disable3Fun.exe  
ModTime: Tue Oct 23 19:44:06 2012 Z

C:\WINDOWS\system32\oobe\windeploy.exe  
ModTime: Sun Nov 21 03:24:24 2010 Z  
Executed

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe  
ModTime: Thu Sep 24 12:40:42 2015 Z  
Executed

C:\Windows\Installer\{2902B717-BEF7-4444-BE28-4C53F902B3B2}\ProductIcon.exe  
ModTime: Sat Feb 20 01:50:08 2016 Z

C:\WINDOWS\SysWOW64\SetIEInstalledDate.exe  
ModTime: Tue Dec 29 19:21:35 2015 Z  
Executed

C:\WINDOWS\Installer\MSI77F1.tmp  
ModTime: Mon Apr 18 15:56:58 2016 Z  
Executed

C:\Windows\system32\wuapp.exe  
ModTime: Fri Nov 20 18:54:15 2015 Z

C:\WINDOWS\System32\wsqmcons.exe  
ModTime: Sun Nov 21 03:24:49 2010 Z  
Executed

C:\Program Files (x86)\Nuance\PDF Viewer Plus\RegistryController.exe  
ModTime: Sat Mar 6 00:11:04 2010 Z  
Executed

C:\WINDOWS\Installer\MSIC9B3.tmp  
ModTime: Mon Apr 18 15:58:25 2016 Z

## SYSTEM OUTPUT

Executed

C:\Program Files\WinRAR\RarExt.dll  
ModTime: Sun Dec 1 18:09:01 2013 Z

C:\\_SMSTaskSequence\Packages\FDA0007A\reg\_win7.exe  
ModTime: Tue Jul 14 01:39:29 2009 Z  
Executed

C:\Program Files\Windows Media Player\WMPNSSUI.dll  
ModTime: Tue Jul 14 01:41:57 2009 Z

C:\Windows\SysWOW64\SearchFolder.dll  
ModTime: Sun Nov 21 03:23:54 2010 Z

C:\Windows\System32\slui.exe  
ModTime: Sun Nov 21 03:24:16 2010 Z  
Executed

C:\Program Files\Windows Media Player\wmpnetwk.exe  
ModTime: Sun Nov 21 03:25:05 2010 Z  
Executed

C:\Program Files\HP\HP Photosmart 7520 series\Bin\HP Photosmart 7520 series.exe  
ModTime: Wed Oct 17 08:39:59 2012 Z  
Executed

C:\Windows\system32\wbem\WMIADAP.EXE  
ModTime: Tue Jul 14 01:39:55 2009 Z  
Executed

c:\users\abe-ar~1\appdata\local\temp\perstemp\29729\download\_files\default\mmi\uninst.exe  
ModTime: Fri Sep 4 14:57:56 2015 Z  
Executed

C:\WINDOWS\SysWOW64\lodctr.exe  
ModTime: Tue Jul 14 01:14:22 2009 Z  
Executed

C:\WINDOWS\SysWOW64\wevtutil.exe  
ModTime: Tue Jul 14 01:14:44 2009 Z  
Executed

C:\WINDOWS\TEMP\mfe30C.tmp\cleanup.exe  
ModTime: Wed Mar 9 14:53:55 2016 Z  
Executed

## SYSTEM OUTPUT

C:\Windows\TEMP\015310~1.EXE

ModTime: Fri Nov 27 14:49:14 2015 Z

Executed

C:\WINDOWS\ccmcache\6\Add\_Admins.BAT

ModTime: Mon Jun 11 14:44:08 2012 Z

C:\Program Files\Common Files\McAfee\UPDMGR\3.0.8053.4\mcupdutl.exe

ModTime: Thu Mar 3 15:27:24 2016 Z

Executed

C:\Program Files (x86)\Common Files\McAfee\DATReputation\mcdatarep.exe

ModTime: Mon Jan 25 15:20:08 2016 Z

Executed

C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe

ModTime: Fri Feb 12 15:10:27 2016 Z

Executed

C:\Program Files (x86)\Nuance\PDF Viewer Plus\pdfPro5Hook.exe

ModTime: Sat Mar 6 01:11:30 2010 Z

Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\x64\scan64.exe

ModTime: Thu Jan 16 00:08:00 2014 Z

Executed

C:\WINDOWS\SysWOW64\xcopy.exe

ModTime: Tue Jul 14 01:14:50 2009 Z

Executed

C:\Program Files\Common Files\Deterministic Networks\Common Files\dneinst.exe

ModTime: Sun Nov 16 22:39:43 2008 Z

Executed

c:\ca4fad583f94fa5f60fa4c\Setup.exe

ModTime: Tue Feb 10 09:27:02 2015 Z

Executed

C:\Program Files (x86)\GUM2990.tmp\GoogleUpdate.exe

ModTime: Tue Apr 19 20:40:07 2016 Z

Executed

C:\Users\Abe-Arjun

Malik\AppData\Local\Temp\{5D609291-3685-4AAC-8681-90B08AE8DB8A}\{E98A9C92-E767-475B-8BC6-8780A86DDC72}\BrRemoveYNSvc.exe

ModTime: Fri Aug 26 16:20:20 2011 Z

Executed

## SYSTEM OUTPUT

C:\Windows\SysWOW64\BRRBT00L.EXE  
ModTime: Thu Dec 26 06:35:41 2013 Z  
Executed

C:\Users\Abe-Arjun Malik\Downloads\vkaraoke.exe  
ModTime: Sat Feb 20 02:03:33 2016 Z  
Executed

C:\Windows\system32\WerFault.exe  
ModTime: Tue Jul 14 01:39:51 2009 Z  
Executed

C:\Windows\SysWOW64\DeviceCenter.dll  
ModTime: Sun Nov 21 03:24:02 2010 Z

C:\Users\Abe-Arjun Malik\Downloads\1clickdvdcopysetup6.1.0.6.exe  
ModTime: Fri Apr 8 11:33:18 2016 Z  
Executed

C:\WINDOWS\system32\mpnotify.exe  
ModTime: Tue Jul 14 01:39:20 2009 Z  
Executed

C:\WINDOWS\Installer\MSIA4E8.tmp  
ModTime: Wed Apr 20 12:59:12 2016 Z  
Executed

C:\Windows\System32\svchost.exe  
ModTime: Sat Nov 29 16:09:44 2014 Z  
Executed

C:\WINDOWS\system32\SearchIndexer.exe  
ModTime: Wed May 4 05:19:28 2011 Z  
Executed

C:\Windows\Temp\nsw1E82.tmp\FilestoInstall\PEFHelper.exe  
ModTime: Mon Dec 14 09:33:24 2015 Z  
Executed

C:\WINDOWS\system32\consent.exe  
ModTime: Thu Jun 25 10:06:15 2015 Z  
Executed

C:\Users\Nikita\AppData\Local\Google\Chrome\User  
Data\SwReporter\5.39.1\software\_reporter\_tool.exe  
ModTime: Tue Dec 1 18:47:49 2015 Z  
Executed



## SYSTEM OUTPUT

C:\Windows\Temp\nseF422.tmp\FilestoInstall\PEFHelper.exe

ModTime: Mon Dec 14 09:33:24 2015 Z

Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Designer 9.0\FormDesigner.exe

ModTime: Fri Oct 8 20:10:48 2010 Z

Executed

C:\Program Files (x86)\Nuance\PaperPort\NuanceWDS.exe

ModTime: Tue Aug 2 21:46:42 2011 Z

Executed

C:\WINDOWS\system32\winsat.exe

ModTime: Sun Nov 21 03:24:35 2010 Z

Executed

C:\Users\Abe-Arjun Malik\Downloads\install\MFC-9340CDW\Setup.exe

ModTime: Fri Sep 14 04:15:27 2012 Z

Executed

C:\\_SMSTaskSequence\Packages\PS10018C\Uninst.exe

ModTime: Thu Jan 16 00:08:00 2014 Z

Executed

C:\Users\Abe-Arjun Malik\Downloads\wpsetup.exe

ModTime: Sat Feb 20 13:25:53 2016 Z

Executed

C:\Program Files (x86)\McAfee\Common Framework\macmnsvc.exe

ModTime: Wed Sep 23 23:57:26 2015 Z

Executed

C:\Program Files\DellTPad\HidFind.exe

ModTime: Thu Apr 16 19:14:31 2015 Z

Executed

C:\WINDOWS\CCM\UpdateTrustedSites.exe

ModTime: Tue Apr 14 08:00:00 2015 Z

Executed

C:\ProgramData\McAfee\Common

Framework\Current\EPOAGENT3000\Install\0409\FramePkg.exe

ModTime: Wed Apr 20 13:18:06 2016 Z

Executed

C:\Program Files (x86)\Nuance\PaperPort\PPnt.exe

ModTime: Tue Aug 2 21:48:44 2011 Z

## SYSTEM OUTPUT

C:\WINDOWS\Installer\MSIB784.tmp  
ModTime: Mon Apr 18 15:57:15 2016 Z  
Executed

C:\Users\Abe-Arjun Malik\Downloads\MFC-9340CDW-inst-B1-US3.EXE  
ModTime: Tue Feb 2 00:46:44 2016 Z  
Executed

C:\WINDOWS\TEMP\mfe41FF.tmp\cleanup.exe  
ModTime: Thu Jun 11 17:12:44 2015 Z  
Executed

C:\PROGRA~2\MICROS~2\Office14\OUTLOOK.EXE  
ModTime: Sat Dec 12 03:20:21 2015 Z  
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\MSIPatchRegFix-AMD64.exe  
ModTime: Thu Mar 10 21:00:19 2016 Z  
Executed

C:\Program Files\McAfee\MSC\mispreg.exe  
ModTime: Thu Dec 3 20:15:56 2015 Z  
Executed

C:\WINDOWS\ccmsetup\vcredist\_x64.exe  
ModTime: Tue Apr 14 06:47:12 2015 Z  
Executed

C:\Users\Abe-Arjun  
Malik\AppData\Local\Adobe\979B5697-E226-44C9-8D79-6E5D76AFED00\gccheck\_small.exe  
ModTime: Thu Jan 7 22:17:08 2016 Z  
Executed

C:\Program Files (x86)\Google\Update\1.3.28.15\GoogleUpdateComRegisterShell64.exe  
ModTime: Tue Apr 19 20:40:07 2016 Z  
Executed

C:\Windows\system32\taskeng.exe  
ModTime: Sun Nov 21 03:24:27 2010 Z  
Executed

C:\PROGRA~1\McAfee\MSC\McInfo.exe  
ModTime: Fri Jan 8 17:44:38 2016 Z  
Executed

C:\WINDOWS\TEMP\mfe30C.tmp\FrmInst.exe  
ModTime: Wed Mar 9 14:53:55 2016 Z

## SYSTEM OUTPUT

Executed

C:\Program Files\Common  
Files\McAfee\AMContent\scanners\x86\_64\datrep\54.0\mcdatarep.exe  
ModTime: Wed Feb 17 00:26:01 2016 Z  
Executed

C:\Program Files\Microsoft Policy Platform\policyHost.exe  
ModTime: Thu Aug 2 16:24:32 2012 Z  
Executed

C:\Program Files (x86)\NCH Software\WavePad\wavepad.exe  
ModTime: Fri Feb 5 14:17:26 2016 Z  
Executed

C:\Windows\system32\net1.exe  
ModTime: Sun Nov 21 03:24:16 2010 Z

C:\Program Files\Common Files\McAfee\Platform\McPltCmd.exe  
ModTime: Tue Nov 3 01:38:14 2015 Z  
Executed

C:\WINDOWS\SysWOW64\msiexec.exe  
ModTime: Mon Jun 15 21:42:49 2015 Z  
Executed

C:\Program Files (x86)\Google\Chrome\Application\48.0.2564.97\Installer\setup.exe  
ModTime: Fri Jan 29 01:23:03 2016 Z  
Executed

C:\WINDOWS\system32\cscript.exe  
ModTime: Sat Oct 12 01:15:48 2013 Z  
Executed

C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleUpdateSetup.exe  
ModTime: Thu Feb 4 14:13:21 2016 Z

C:\ProgramData\dell\drivers\multiplatform\_bios\_btrfstboot\x86\_64\HAPI\hapint.exe  
ModTime: Fri Sep 27 05:56:29 2013 Z  
Executed

C:\Program Files  
(x86)\McAfee\SiteAdvisor\{C0D0029B-8FFE-4540-B398-1CE31FEABB7D}\saInst.exe  
ModTime: Thu Feb 25 18:11:07 2016 Z  
Executed

C:\Windows\TEMP\7A195C44-AA01-465B-A17D-7D9EF2300C86\dismhost.exe  
ModTime: Sat Nov 29 16:13:49 2014 Z

## SYSTEM OUTPUT

Executed

C:\WINDOWS\TEMP\{D2B9C003-A3CD-44A0-9DE5-52FE986C03E5}\setlicense.exe

ModTime: Mon Apr 18 16:00:10 2016 Z

Executed

C:\WINDOWS\system32\PING.EXE

ModTime: Tue Jul 14 01:14:28 2009 Z

C:\Program Files (x86)\internet explorer\iexplore.exe

ModTime: Tue Dec 29 19:21:35 2015 Z

Executed

C:\Windows\Installer\{5FDC06BF-3D3D-4367-8FFB-4FAFCB61972D}\Icon09DB8A85.exe

ModTime: Mon Apr 18 15:56:59 2016 Z

C:\Windows\System32\takeown.exe

ModTime: Sun Nov 21 03:23:55 2010 Z

C:\\_SMSTaskSequence\Packages\PS10018C\SetupVSE.Exe

ModTime: Thu Jan 16 00:08:00 2014 Z

Executed

C:\Windows\SysWOW64\plugincpl13122.cpl

ModTime: Tue Apr 5 08:38:20 2005 Z

C:\Windows\SysWOW64\plugincpl13113.cpl

ModTime: Thu May 8 18:35:36 2003 Z

C:\Users\Nikita\AppData\Local\Microsoft\Windows\Burn\Burn\WLAN\_Broadcom\_Win7\_64\_VER630223215\setup.exe

ModTime: Thu Jan 16 17:47:50 2014 Z

C:\Program Files\Common Files\McAfee\ModuleCore\ModuleCoreReg.exe

ModTime: Wed Jan 6 19:32:56 2016 Z

Executed

C:\\_SMSTaskSequence\Packages\FDA0020E\Java\_Inst.CMD

ModTime: Thu May 2 14:38:43 2013 Z

C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleCrashHandler64.exe

ModTime: Thu Feb 4 14:13:21 2016 Z

Executed

C:\WINDOWS\SysWOW64\wbem\WMIC.exe

ModTime: Tue Jul 14 01:14:46 2009 Z

Executed

## SYSTEM OUTPUT

C:\Program Files (x86)\Windows Sidebar\sbdrop.dll  
ModTime: Tue Jul 14 01:16:13 2009 Z

C:\Program Files (x86)\McAfee\SiteAdvisor\Download\s7sk.11.exe  
ModTime: Fri Mar 4 21:19:16 2016 Z  
Executed

C:\Windows\SoftwareDistribution\Download\Install\GWXWU\_1.exe  
ModTime: Sat Feb 20 00:11:49 2016 Z  
Executed

G:\Setup.exe  
ModTime: Fri Jan 16 08:14:08 2009 Z

C:\WINDOWS\SysWOW64\unlodctr.exe  
ModTime: Sun Nov 21 03:24:01 2010 Z  
Executed

C:\Program Files (x86)\Microsoft Office\Office14\msotmed.exe  
ModTime: Tue Dec 18 03:47:23 2012 Z  
Executed

C:\Program Files (x86)\McAfee\SiteAdvisor\McSACore.exe  
ModTime: Wed Dec 2 15:38:45 2015 Z  
Executed

C:\Users\Abe-Arjun Malik\AppData\Local\Apple\Apple Software  
Update\QuickTimeInstallerAdmin.exe  
ModTime: Thu Jan 7 22:06:09 2016 Z  
Executed

C:\WINDOWS\TEMP\InstallPlugin\_21\_0\_0\_182.exe  
ModTime: Mon Mar 7 20:52:56 2016 Z  
Executed

C:\Program Files (x86)\Microsoft Office\Office12\CLVIEW.EXE  
ModTime: Wed Jul 27 10:13:32 2011 Z  
Executed

C:\Windows\SoftwareDistribution\Download\Install\Windows-KB890830-x64-V5.32-delta.exe  
ModTime: Fri Jan 8 20:43:38 2016 Z  
Executed

C:\Program Files (x86)\Brother\PcFaxTx\PCFaxTxDial.exe  
ModTime: Fri Dec 7 19:44:52 2012 Z  
Executed

## SYSTEM OUTPUT

C:\WINDOWS\system32\DRIVERS\o2flash.exe  
ModTime: Thu Apr 16 19:14:31 2015 Z  
Executed

C:\Windows\system32\GWX\GWXConfigManager.exe  
ModTime: Tue Dec 8 19:06:56 2015 Z  
Executed

C:\WINDOWS\CCM\TsManager.exe  
ModTime: Tue Apr 14 08:00:00 2015 Z  
Executed

C:\Program Files\HP\HP Photosmart 7520 series\bin\HPNetworkCommunicator.exe  
ModTime: Wed Oct 17 08:29:59 2012 Z  
Executed

C:\WINDOWS\System32\taskkill.exe  
ModTime: Tue Jul 14 01:39:47 2009 Z  
Executed

C:\Windows\Microsoft.NET\Framework\v4.0.30319\regtlibv12.exe  
ModTime: Sat Apr 12 04:08:05 2014 Z  
Executed

C:\Windows\Microsoft.NET\Framework\v2.0.50727\cvtres.exe  
ModTime: Sat Nov 29 16:52:45 2014 Z  
Executed

C:\WINDOWS\CCM\TSMBootstrap.exe  
ModTime: Fri May 8 04:59:59 2015 Z  
Executed

C:\Users\Nikita\Downloads\SmartGesture\_Win7\_64\_VER2214\Disable3Fun.exe  
ModTime: Tue Oct 23 19:44:06 2012 Z

C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleCrashHandler.exe  
ModTime: Thu Feb 4 14:13:21 2016 Z  
Executed

C:\WINDOWS\system32\net1.exe  
ModTime: Sun Nov 21 03:24:07 2010 Z  
Executed

D:\Prerequisites\fixesd.bat  
ModTime: Mon Oct 19 18:27:11 2015 Z

C:\Program Files (x86)\Cisco Systems\Cisco Jabber\CiscoJabber.exe  
ModTime: Thu Aug 7 23:05:34 2014 Z

## SYSTEM OUTPUT

C:\Program Files\Common Files\McAfee\ClientAnalytics\CATracker.exe  
 ModTime: Tue Nov 24 17:06:00 2015 Z  
 Executed

C:\Windows\splwow64.exe  
 ModTime: Sat Nov 29 16:06:19 2014 Z  
 Executed

C:\Windows\TEMP\CF9E0F01-CA5F-494C-BC14-5843000ED221\dismhost.exe  
 ModTime: Sat Nov 29 16:13:49 2014 Z  
 Executed

C:\Program Files\Windows Media Player\wmpshare.exe  
 ModTime: Wed Apr 29 18:21:29 2015 Z  
 Executed

C:\Windows\SysWOW64\PhotoMetadataHandler.dll  
 ModTime: Tue Jul 14 01:16:12 2009 Z

C:\Program Files  
 (x86)\McAfee\SiteAdvisor\{A80DB781-A37F-416A-8311-0413A1FD2020}\saInst.exe  
 ModTime: Mon Mar 21 16:18:30 2016 Z  
 Executed

C:\ProgramData\webex\WebEx\1530\atasinst.exe  
 ModTime: Fri Sep 11 08:19:50 2015 Z  
 Executed

C:\\_SMSTaskSequence\Packages\FDA002C1\reg\_64.exe  
 ModTime: Tue Jul 14 01:39:30 2009 Z  
 Executed

C:\WINDOWS\SysWOW64\net1.exe  
 ModTime: Sun Nov 21 03:24:16 2010 Z  
 Executed

C:\\_SMSTaskSequence\Packages\FDA002D5\certmgr.exe  
 ModTime: Tue Jan 30 01:07:56 2001 Z  
 Executed

c:\program files (x86)\common files\mcafee\installer\9.0.6002.0\mcinst.exe  
 ModTime: Wed Oct 28 20:05:58 2015 Z  
 Executed

C:\Users\Nikita\Downloads\,northsouth,3563805613,-1031684194,TC,0-0,SDJTSwAAAAKEIYI1  
 XIcej435gFMQsDqBrEKL3vahWSXXdXH8K-Fn6A2\_webex.exe  
 ModTime: Sun Jan 31 16:05:19 2016 Z

## SYSTEM OUTPUT

C:\Windows\System32\mobsync.exe  
ModTime: Sun Nov 21 03:24:51 2010 Z  
Executed

C:\WINDOWS\WinSxS\amd64\_microsoft-windows-ie-pdm\_31bf3856ad364e35\_8.0.7600.16385\_non  
e\_6425238b793ee910\PDMSSetup.exe  
ModTime: Tue Jul 14 01:39:26 2009 Z  
Executed

C:\WINDOWS\TEMP\mfe41FF.tmp\FrmInst.exe  
ModTime: Thu Jun 11 17:12:44 2015 Z  
Executed

C:\Users\Abe-Arjun  
Malik\AppData\Local\Temp\{5D609291-3685-4AAC-8681-90B08AE8DB8A}\{E98A9C92-E767-475B-  
8BC6-8780A86DDC72}\BrRemPnP.exe  
ModTime: Tue Aug 28 22:06:10 2012 Z  
Executed

c:\PROGRA~2\mcafee\SITEAD~1\sau1.exe  
ModTime: Tue Dec 29 20:56:48 2015 Z  
Executed

c:\program files (x86)\common files\mcafee\installer\9.0.7003.0\mcinst.exe  
ModTime: Fri Nov 27 14:49:14 2015 Z  
Executed

C:\Windows\SysWOW64\net.exe  
ModTime: Tue Jul 14 01:14:27 2009 Z  
Executed

C:\WINDOWS\SysWOW64\HOSTNAME.EXE  
ModTime: Tue Jul 14 01:14:21 2009 Z  
Executed

C:\Program Files\Common Files\McAfee\AMCore\mcshield.exe  
ModTime: Mon Sep 28 12:03:16 2015 Z  
Executed

C:\WINDOWS\system32\DrvInst.exe  
ModTime: Tue Jul 14 01:39:07 2009 Z  
Executed

C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\ngen.exe  
ModTime: Thu Mar 18 18:27:13 2010 Z  
Executed



## SYSTEM OUTPUT

C:\Windows\System32\wpdshext.dll  
ModTime: Thu Jan 29 03:19:34 2015 Z

C:\WINDOWS\system32\HOSTNAME.EXE  
ModTime: Tue Jul 14 01:39:12 2009 Z  
Executed

C:\Windows\system32\regsvr32.exe  
ModTime: Tue Jul 14 01:14:30 2009 Z  
Executed

C:\\_SMSTaskSequence\Packages\FDA000DB\install\_all.CMD  
ModTime: Fri Feb 25 19:04:56 2011 Z

C:\ProgramData\webex\WebEx\500\nbrplay.exe  
ModTime: Fri Sep 11 08:19:58 2015 Z  
Executed

C:\WINDOWS\system32\mspaint.exe  
ModTime: Tue Jul 14 01:39:24 2009 Z

C:\Windows\system32\vssvc.exe  
ModTime: Sun Nov 21 03:23:55 2010 Z  
Executed

C:\Users\Abe-Arjun  
Malik\AppData\Local\Adobe\979B5697-E226-44C9-8D79-6E5D76AFED00\gtcheck.exe  
ModTime: Thu Jan 7 22:17:09 2016 Z  
Executed

c:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\ServiceModelReg.exe  
ModTime: Wed May 28 12:20:39 2014 Z  
Executed

C:\Program Files\Common Files\AV\McAfee Anti-Virus And Anti-Spyware\upgrade.exe  
ModTime: Tue Nov 3 21:35:52 2015 Z  
Executed

C:\Program Files\Common Files\McAfee\Platform\Core\mchost.exe  
ModTime: Tue Nov 3 00:53:26 2015 Z  
Executed

C:\Windows\SoftwareDistribution\Download\Install\ndp45-kb3135996-x64.exe  
ModTime: Thu Feb 18 20:26:03 2016 Z  
Executed

C:\Program Files (x86)\Nuance\PDF Create 8\PdfCreate8Hook.exe  
ModTime: Wed Jun 13 12:10:00 2012 Z

## SYSTEM OUTPUT

Executed

C:\Program Files (x86)\McAfee\SiteAdvisor\Download\s2s8.u.exe  
ModTime: Thu Mar 24 19:41:10 2016 Z  
Executed

C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleUpdateComRegisterShell64.exe  
ModTime: Thu Feb 4 14:13:21 2016 Z  
Executed

C:\\_SMSTaskSequence\Packages\FDA000DB\jinit13122\Setup.exe  
ModTime: Wed Sep 5 10:23:24 2001 Z  
Executed

C:\Program Files (x86)\Common Files\Adobe\Calibration\Adobe Gamma Loader.exe  
ModTime: Tue Aug 6 18:37:49 2002 Z  
Executed

C:\Program Files (x86)\Mozilla Firefox\plugin-container.exe  
ModTime: Thu Jan 7 15:35:45 2016 Z  
Executed

C:\WINDOWS\TEMP\vcredist\_x64\_2010.exe  
ModTime: Fri Nov 22 19:59:18 2013 Z  
Executed

C:\Program Files\Common Files\McAfee\ClientAnalytics\McClientAnalytics.exe  
ModTime: Tue Nov 24 17:06:10 2015 Z  
Executed

C:\WINDOWS\system32\DllHost.exe  
ModTime: Tue Jul 14 01:39:06 2009 Z  
Executed

c:\PROGRA~1\mcafee\VIRUSS~1\mcvsshld.exe  
ModTime: Tue Oct 20 23:13:32 2015 Z  
Executed

C:\Program Files (x86)\GUMDA54.tmp\GoogleUpdate.exe  
ModTime: Wed Jan 13 23:14:37 2016 Z  
Executed

C:\Program Files (x86)\Common Files\InstallShield\Engine\6\Intel 32\IKernel.exe  
ModTime: Wed Sep 5 07:24:00 2001 Z  
Executed

C:\ProgramData\FLEXnet\Connect\11\ISDM.exe  
ModTime: Tue May 5 21:06:03 2009 Z

## SYSTEM OUTPUT

C:\Program Files (x86)\Google\Chrome\Application\48.0.2564.109\Installer\setup.exe  
ModTime: Thu Feb 11 12:52:51 2016 Z  
Executed

C:\Program Files\ActivIdentity\ActivClient\acevents.exe  
ModTime: Wed Jun 3 21:38:32 2009 Z  
Executed

C:\PROGRA~3\WebEx\WebEx\T30\_TC\atmgr.exe  
ModTime: Sun Jan 31 16:06:45 2016 Z  
Executed

C:\Program Files  
(x86)\McAfee\SiteAdvisor\{87C58462-EF7A-4930-9752-30714CAF5746}\saInst.exe  
ModTime: Mon Mar 21 16:18:30 2016 Z  
Executed

C:\Program Files (x86)\Google\Update\1.3.28.15\GoogleCrashHandler.exe  
ModTime: Tue Apr 19 20:40:07 2016 Z  
Executed

C:\WINDOWS\SysWOW64\WindowsPowerShell\v1.0\powershell.exe  
ModTime: Tue Jul 14 01:14:24 2009 Z  
Executed

C:\WINDOWS\TEMP\7DBA53D1-D0AF-46C3-8392-AE67C4DD47F9\dismhost.exe  
ModTime: Fri May 30 08:07:49 2014 Z  
Executed

C:\Windows\System32\tabcsl.exe  
ModTime: Sun Nov 21 03:24:33 2010 Z

C:\Windows\system32\atieclxx.exe  
ModTime: Thu Sep 12 02:47:48 2013 Z  
Executed

C:\WINDOWS\Installer\MSI49C3.tmp  
ModTime: Tue Apr 19 20:41:21 2016 Z  
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\msipatchregfix-amd64.exe  
ModTime: Thu Mar 10 21:02:43 2016 Z  
Executed

D:\start.exe  
ModTime: Thu May 17 02:56:34 2012 Z

## SYSTEM OUTPUT

C:\Program Files (x86)\Microsoft Office\Office14\MAPISHELL.DLL  
 ModTime: Wed May 16 10:37:55 2012 Z

C:\\_SMSTaskSequence\Packages\FDA0004E\Java\_1.6\_17.cmd  
 ModTime: Fri Jun 15 13:15:07 2012 Z

C:\WINDOWS\SysWOW64\rundll32.exe  
 ModTime: Tue Jul 14 01:14:31 2009 Z  
 Executed

C:\Users\Nikita\AppData\Local\Microsoft\Windows\Burn\Burn\WLAN\_Atheros\_Win7\_64\_VER10  
 00285\setup.exe  
 ModTime: Mon Mar 3 19:51:51 2014 Z

C:\Program Files\HP\HP Photosmart 7520 series\Bin\HPScanDisco.exe  
 ModTime: Wed Oct 17 08:27:05 2012 Z  
 Executed

C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe  
 ModTime: Thu Mar 20 22:50:31 2014 Z  
 Executed

C:\Windows\SysWOW64\shdocvw.dll  
 ModTime: Sat Nov 29 16:12:06 2014 Z

C:\Program Files (x86)\McAfee\SiteAdvisor\Download\s3uo.v.exe  
 ModTime: Thu Feb 18 16:20:16 2016 Z  
 Executed

C:\Windows\system32\wormgr.exe  
 ModTime: Tue Jul 14 01:39:51 2009 Z  
 Executed

C:\WINDOWS\TEMP\{F2FCE38B-19E6-4FA0-A321-9765C6FE32D3}\InstallFlashPlayer.exe  
 ModTime: Mon Apr 18 15:45:11 2016 Z  
 Executed

C:\Windows\Installer\{90140000-0011-0000-0000-0000000FF1CE}\pptico.exe  
 ModTime: Wed Dec 30 12:57:23 2015 Z

C:\Program Files\FDA\Utils\WSAP.exe  
 ModTime: Tue Nov 15 15:04:38 2011 Z  
 Executed

C:\Users\Abe-Arjun  
 Malik\AppData\Local\Temp\{5D609291-3685-4AAC-8681-90B08AE8DB8A}\{E98A9C92-E767-475B-  
 8BC6-8780A86DDC72}\BrWiEvRg.exe  
 ModTime: Fri May 13 20:30:57 2011 Z

## SYSTEM OUTPUT

Executed

C:\Program Files\Common Files\McAfee\CSP\1.8.203.0\McCSPServiceHost.exe

ModTime: Wed Dec 2 15:05:12 2015 Z

Executed

C:\Windows\system32\lsmd.exe

ModTime: Sun Nov 21 03:23:53 2010 Z

Executed

C:\Program Files (x86)\Google\Chrome\Application\50.0.2661.75\Installer\chromstp.exe

ModTime: Tue Apr 19 20:40:55 2016 Z

Executed

C:\Program Files (x86)\McAfee.com\Agent\mcagent.exe

ModTime: Thu Dec 3 20:15:20 2015 Z

C:\WINDOWS\ccmcache\2\ciscoanyconnect\_copy\_fdauseripsecprof.cmd

ModTime: Fri Apr 10 16:59:10 2015 Z

C:\Program Files\Microsoft Silverlight\5.1.41212.0\coregen.exe

ModTime: Sat Dec 12 04:42:26 2015 Z

Executed

C:\WINDOWS\system32\findstr.exe

ModTime: Sun Nov 21 03:24:08 2010 Z

Executed

C:\Windows\System32\tskill.exe

ModTime: Sun Nov 21 03:24:41 2010 Z

C:\Users\Abe-Arjun Malik\Downloads\KantoPlayer(1).exe

ModTime: Sun Feb 14 15:57:08 2016 Z

C:\Program Files (x86)\McAfee\Common Framework\x86\UpdaterUI.exe

ModTime: Thu Sep 24 00:04:50 2015 Z

Executed

C:\Program Files (x86)\ControlCenter4\BrCcBoot.exe

ModTime: Mon Nov 19 21:25:14 2012 Z

Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\x64\shext.dll

ModTime: Thu Jan 16 00:08:00 2014 Z

C:\Windows\System32\tscon.exe

ModTime: Sun Nov 21 03:24:41 2010 Z

## SYSTEM OUTPUT

C:\Windows\TEMP\196F2278-896D-4E04-90AD-6CA460E795E2\dismhost.exe  
ModTime: Sat Nov 29 16:13:49 2014 Z  
Executed

C:\WINDOWS\Installer\MSIC5D8.tmp  
ModTime: Mon Apr 18 15:58:24 2016 Z  
Executed

C:\WINDOWS\SYSTEM32\SETUPUGC.EXE  
ModTime: Tue Jul 14 01:39:39 2009 Z  
Executed

C:\WINDOWS\SysWOW64\net.exe  
ModTime: Tue Jul 14 01:14:27 2009 Z  
Executed

C:\Windows\SysWOW64\regedit.exe  
ModTime: Tue Jul 14 01:14:30 2009 Z  
Executed

C:\Windows\SysWOW64\lodctr.exe  
ModTime: Tue Jul 14 01:14:22 2009 Z  
Executed

C:\Program Files\McAfee\Host Intrusion Prevention\ClientControl.exe  
ModTime: Thu Jun 25 01:34:12 2015 Z  
Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\DLG\exe\43e5c49e9d25cd3e3378fe036281f011\compet  
e\_032415013024.exe  
ModTime: Sat Feb 20 01:45:56 2016 Z  
Executed

C:\Windows\system32\lodctr.exe  
ModTime: Tue Jul 14 01:39:15 2009 Z  
Executed

C:\WINDOWS\WinSxS\amd64\_microsoft-windows-ie-gc-registeriepkeys\_31bf3856ad364e35\_11.  
2.9600.16428\_none\_0a3fe92b38dd8c45\RegisterIEPKEYs.exe  
ModTime: Tue Dec 29 19:21:35 2015 Z  
Executed

C:\Program Files (x86)\McAfee\Common Framework\McScript\_InUse.exe  
ModTime: Tue Feb 10 20:07:59 2015 Z  
Executed

C:\Program Files\DellTPad\Apntex.exe  
ModTime: Thu Apr 16 19:14:31 2015 Z

## SYSTEM OUTPUT

Executed

C:\Program Files\NVIDIA Corporation\Display\nvtray.exe

ModTime: Tue Nov 4 01:04:32 2014 Z

Executed

C:\WINDOWS\system32\scrnsave.scr

ModTime: Tue Jul 14 01:38:53 2009 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\WavePad-7716-1\switchsetup.exe

ModTime: Sat Feb 20 13:29:10 2016 Z

Executed

C:\Windows\System32\cryptext.dll

ModTime: Tue Jul 14 01:40:24 2009 Z

C:\Windows\System32\taskkill.exe

ModTime: Tue Jul 14 01:39:47 2009 Z

C:\Users\Nikita\Downloads\Cisco\_WebEx\_Add-On.exe

ModTime: Sun Jan 31 16:05:40 2016 Z

C:\Users\AD\_DCC~1.NCH\AppData\Local\Temp\DMT\_Files\USMT\USMTRestore.exe

ModTime: Thu Jul 31 04:37:51 2014 Z

Executed

D:\paperport\Prerequisite\System64\vcredist\_x64.exe

ModTime: Mon Jun 18 06:43:57 2012 Z

C:\Windows\SysWOW64\rundll32.exe

ModTime: Tue Jul 14 01:14:31 2009 Z

Executed

C:\Program Files

(x86)\McAfee\SiteAdvisor\{2251B01E-9847-4E97-A8BF-FE932C84BCF9}\mcinst.exe

ModTime: Mon May 4 19:41:42 2015 Z

Executed

C:\WINDOWS\TEMP\\_ISTMP1.DIR\\_ISTMP0.DIR\uncrunch.exe

ModTime: Thu May 8 18:37:26 2003 Z

Executed

C:\Program Files\iTunes\iTunes.exe

ModTime: Thu Aug 13 06:43:00 2015 Z

Executed

C:\WINDOWS\Installer\MSI5817.tmp

## SYSTEM OUTPUT

ModTime: Tue Apr 19 20:41:24 2016 Z  
Executed

C:\WINDOWS\WinSxS\amd64\_microsoft-windows-i..eoptionalcomponents\_31bf3856ad364e35\_11  
.2.9600.16428\_none\_e410f56f6c4ee930\ConfigureIEOptionalComponents.exe  
ModTime: Tue Dec 29 19:21:35 2015 Z  
Executed

C:\Windows\System32\sysmain.dll  
ModTime: Wed Jul 15 18:09:18 2015 Z

C:\Program Files (x86)\McAfee\Common Framework\NaPrdMgr.exe  
ModTime: Tue Feb 10 20:07:59 2015 Z  
Executed

C:\Users\Nikita\AppData\Local\Microsoft\Windows\Burn\Burn\Audio\_Realtek\_Win7\_64\_VER6  
017213\ChCfg.exe  
ModTime: Wed Feb 9 19:56:00 2011 Z

C:\DMTFiles\CDMReport.exe  
ModTime: Thu May 22 21:40:08 2014 Z  
Executed

C:\Users\AD\_DCC~1\NCH\AppData\Local\Temp\CDM\_Files\CDMUpdate\_X64.exe  
ModTime: Thu May 22 21:21:39 2014 Z  
Executed

C:\WINDOWS\Installer\MSICD1D.tmp  
ModTime: Mon Apr 18 15:58:26 2016 Z  
Executed

C:\Program Files\Internet Explorer\iexplore.exe  
ModTime: Wed Nov 11 21:12:58 2015 Z  
Executed

C:\progra~2\java\jre-1.6.38\bin\javaw.exe  
ModTime: Mon Apr 18 15:54:25 2016 Z  
Executed

C:\Program Files (x86)\Java\jre6\bin\unpack200.exe  
ModTime: Mon Apr 18 15:54:07 2016 Z  
Executed

C:\Windows\System32\networkexplorer.dll  
ModTime: Sun Nov 21 03:24:02 2010 Z

C:\Program Files\Tracker Software\PDF Viewer\PDFXCview.exe  
ModTime: Wed Sep 9 03:09:36 2015 Z



## SYSTEM OUTPUT

Executed

C:\WINDOWS\WinSxS\amd64\_microsoft-windows-i...-setieinstalleddate\_31bf3856ad364e35\_11.2.9600.16428\_none\_eace14b8d6178cca\SetIEInstalledDate.exe

ModTime: Tue Dec 29 19:21:35 2015 Z

Executed

C:\WINDOWS\SysWOW64\wbem\mofcomp.exe

ModTime: Tue Jul 14 01:14:24 2009 Z

Executed

C:\Program Files (x86)\Windows Media Player\setup\_wm.exe

ModTime: Sun Nov 21 03:25:10 2010 Z

Executed

C:\WINDOWS\system32\lsass.exe

ModTime: Tue Oct 20 01:04:53 2015 Z

Executed

C:\Windows\twain\_32\TWAINSP\_HP.ds

ModTime: Tue Jun 16 11:36:56 2015 Z

C:\Users\Abe-Arjun

Malik\AppData\Local\Adobe\4C8BAB87-784D-4819-8C69-19F593639E7B\99F7C92F-ECBB-487A-8600-FDFF3D4098E1\1EEA925A-A58C-4E30-A5AA-2D8646F0D25F

ModTime: Sat Feb 6 20:05:47 2016 Z

Executed

C:\Program Files (x86)\Kanto Player\KantoPlayer.exe

ModTime: Sun Dec 13 23:19:03 2015 Z

Executed

C:\WINDOWS\TEMP\CR\_08BB0.tmp\setup.exe

ModTime: Wed Apr 20 12:59:18 2016 Z

Executed

C:\Program Files\iTunes\iTunesHelper.exe

ModTime: Thu Aug 13 06:43:12 2015 Z

Executed

C:\Program Files (x86)\Cisco Systems\VPN Client\vpnclient.exe

ModTime: Fri Mar 4 16:46:33 2011 Z

Executed

C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnagent.exe

ModTime: Wed Mar 12 20:52:18 2014 Z

Executed

## SYSTEM OUTPUT

C:\Users\Nikita\AppData\Local\WebEx\ChromeNativeHost\CiscoWebExStart.exe

ModTime: Sun Jan 31 16:06:38 2016 Z

Executed

C:\Program Files (x86)\ControlCenter4\BrCtrlCntr.exe

ModTime: Mon Nov 19 21:24:46 2012 Z

Executed

C:\Windows\system32\wbem\wmiprvse.exe

ModTime: Sun Nov 21 03:24:15 2010 Z

Executed

C:\WINDOWS\CCM\RemCtrl\CmRcService.exe

ModTime: Tue Apr 14 08:00:00 2015 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\\_iu14D2N.tmp

ModTime: Tue Feb 16 01:35:16 2016 Z

Executed

C:\Windows\system32\lsass.exe

ModTime: Tue Oct 20 01:10:48 2015 Z

Executed

C:\Windows\System32\igfxcp1.cpl

ModTime: Thu Mar 20 15:40:18 2014 Z

C:\Windows\System32\StorageContextHandler.dll

ModTime: Tue Jul 14 01:41:54 2009 Z

C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\ServiceModelReg.exe

ModTime: Thu Mar 18 17:16:28 2010 Z

Executed

C:\Windows\helppane.exe

ModTime: Tue Jul 14 01:39:12 2009 Z

Executed

C:\Program Files (x86)\Google\Chrome\Application\47.0.2526.106\Installer\setup.exe

ModTime: Wed Dec 16 22:05:57 2015 Z

Executed

C:\Windows\SoftwareDistribution\Download\Install\Silverlight\_x64.exe

ModTime: Wed Jan 6 22:05:08 2016 Z

Executed

C:\Users\Nikita\Downloads\Cisco\_WebEx\_Add-On (1).exe

ModTime: Sun Jan 31 16:06:24 2016 Z

## SYSTEM OUTPUT

Executed

C:\Windows\system32\lpremove.exe  
ModTime: Tue Jul 14 01:39:16 2009 Z  
Executed

C:\Windows\System32\sdshext.dll  
ModTime: Tue Jul 14 01:41:53 2009 Z

C:\WINDOWS\CCM\Ccm32BitLauncher.exe  
ModTime: Tue Apr 14 08:00:00 2015 Z  
Executed

C:\WINDOWS\Installer\MSI728D.tmp  
ModTime: Mon Apr 18 15:56:57 2016 Z  
Executed

c:\PROGRA~1\COMMON~1\mcafee\mhn\ALERTH~1.EXE  
ModTime: Tue Dec 1 09:47:03 2015 Z  
Executed

C:\WINDOWS\SysWOW64\runonce.exe  
ModTime: Sun Nov 21 03:23:53 2010 Z  
Executed

C:\WINDOWS\system32\xpsrchvw.exe  
ModTime: Tue Jul 14 01:39:59 2009 Z

C:\Windows\TEMP\CR\_0A7DE.tmp\setup.exe  
ModTime: Fri Jan 29 01:23:03 2016 Z  
Executed

C:\Program Files (x86)\Citrix\GoToMeeting\1189\G2MInstaller.exe  
ModTime: Tue Apr 19 20:40:39 2016 Z  
Executed

C:\Windows\System32\msiexec.exe  
ModTime: Mon Jun 15 21:42:49 2015 Z

C:\Program Files  
(x86)\McAfee\SiteAdvisor\{7858331B-FE1D-4ACA-AEC9-F28B9E16A0C4}\saInst.exe  
ModTime: Thu Feb 25 18:11:07 2016 Z  
Executed

C:\Windows\system32\MRT.exe  
ModTime: Thu Jan 14 16:30:30 2016 Z  
Executed

## SYSTEM OUTPUT

C:\Program Files (x86)\Common Files\Microsoft Shared\Ink\TabTip32.exe

ModTime: Tue Sep 1 17:52:16 2015 Z

Executed

C:\Program Files\Common Files\McAfee\MHN\MozyRemove.exe

ModTime: Tue Dec 29 10:29:28 2015 Z

Executed

C:\Windows\Installer\MSI9D1E.tmp

ModTime: Tue Feb 2 00:19:38 2016 Z

Executed

C:\Windows\SysWOW64\extrac32.exe

ModTime: Tue Jul 14 01:14:20 2009 Z

Executed

C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe

ModTime: Thu Apr 16 19:14:29 2015 Z

Executed

C:\Windows\system32\pca lua.exe

ModTime: Tue Feb 3 03:30:36 2015 Z

Executed

C:\Windows\WinSxS\amd64\_microsoft-windows-i..national-timezones\_31bf3856ad364e35\_6.1.7601.23387\_none\_73ae16d839858657\tzupd.exe

ModTime: Fri Mar 11 17:41:11 2016 Z

Executed

C:\\_SMSTaskSequence\Packages\PS1002F4\IE11-Windows6.1-x64-en-us.exe

ModTime: Thu Oct 9 19:38:41 2014 Z

Executed

C:\Program Files (x86)\McAfee\Temp\qxzA615\mccertupd.exe

ModTime: Mon Dec 7 06:06:03 2015 Z

Executed

C:\Program Files (x86)\Common Files\Apple\Mobile Device Support\SyncServer.exe

ModTime: Tue Aug 4 20:05:36 2015 Z

Executed

D:\ChromeSetup (1).exe

ModTime: Fri Oct 2 20:17:22 2015 Z

C:\Users\Abe-Arjun

Malik\AppData\Local\Temp\{5D609291-3685-4AAC-8681-90B08AE8DB8A}\{E98A9C92-E767-475B-8BC6-8780A86DDC72}\BrLogRx.exe

ModTime: Fri Feb 27 21:38:09 2009 Z

## SYSTEM OUTPUT

Executed

C:\PROGRA~3\WebEx\atcliun.exe  
ModTime: Sun Jan 31 16:06:46 2016 Z  
Executed

C:\WINDOWS\SYSTEM32\cmd.exe  
ModTime: Sun Nov 21 03:23:55 2010 Z  
Executed

C:\WINDOWS\system32\Dwm.exe  
ModTime: Tue Jul 14 01:39:08 2009 Z  
Executed

C:\Program Files  
(x86)\McAfee\SiteAdvisor\{AEF1B64A-FB8F-4507-AE22-E91E60B30E39}\mcinst.exe  
ModTime: Mon May 4 19:41:42 2015 Z  
Executed

C:\Program Files\Common Files\McAfee\SystemCore\mcshield.exe  
ModTime: Mon Apr 18 15:58:25 2016 Z  
Executed

C:\WINDOWS\TEMP\{05FCBA67-6D54-49E4-9761-BECFDF93372C}\InstallFlashPlayer.exe  
ModTime: Wed Apr 20 14:56:07 2016 Z  
Executed

C:\WINDOWS\TEMP\{AF27EDE3-3E6E-4DCB-A335-9603668E26D3}\InstallFlashPlayer.exe  
ModTime: Mon Apr 18 15:45:03 2016 Z  
Executed

C:\WINDOWS\system32\igfxTray.exe  
ModTime: Thu Apr 16 19:14:55 2015 Z  
Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\cw.exe  
ModTime: Mon Mar 23 19:59:13 2015 Z  
Executed

C:\Program Files  
(x86)\McAfee\SiteAdvisor\{87C58462-EF7A-4930-9752-30714CAF5746}\mcinst.exe  
ModTime: Mon May 4 19:41:42 2015 Z  
Executed

C:\Windows\system32\WFS.exe  
ModTime: Sun Nov 21 03:25:07 2010 Z  
Executed

## SYSTEM OUTPUT

C:\\_SMSTaskSequence\Packages\PS1002D8\multiplatform\_bios\_btrfstboot.exe

ModTime: Thu Nov 19 19:42:52 2015 Z

Executed

C:\Program Files\Common Files\McAfee\Casper\AmcInst.exe

ModTime: Thu Nov 26 16:52:33 2015 Z

Executed

C:\Windows\SysWOW64\plugincpl13118.cpl

ModTime: Tue Mar 2 18:29:30 2004 Z

C:\WINDOWS\SysWOW64\DllHost.exe

ModTime: Tue Jul 14 01:14:18 2009 Z

Executed

C:\Program Files (x86)\Consumer

Input\Update\Install\{D65C7D84-329C-45FF-8545-40DD7C495423}\cimt-3.2.1-1146.exe

ModTime: Wed Feb 17 21:08:35 2016 Z

Executed

c:\PROGRA~1\mcafee\VIRUSS~1\mcvsmapi.exe

ModTime: Tue Oct 20 23:12:36 2015 Z

Executed

C:\\_SMSTaskSequence\Packages\PS1001E9\CheckPoint\_Install.CMD

ModTime: Thu Jan 22 15:24:32 2015 Z

C:\WINDOWS\system32\regsvr32.exe

ModTime: Tue Jul 14 01:39:29 2009 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\{FA2E8C6E-8B03-40BC-8326-1398BAE13797}\InstallFlashPlayer.exe

ModTime: Thu Jan 28 22:39:43 2016 Z

Executed

C:\WINDOWS\ccmsetup\vc50727\_x64.exe

ModTime: Tue Apr 14 06:47:12 2015 Z

Executed

C:\Program Files (x86)\vanBasco's Karaoke Player\vmidi.exe

ModTime: Thu Mar 11 11:00:00 2004 Z

Executed

C:\Program Files\DVD Maker\DVDMaker.exe

ModTime: Tue Jul 14 01:39:08 2009 Z

C:\Program Files (x86)\Brown02\Brother\BrStMonW.exe

## SYSTEM OUTPUT

ModTime: Tue Jul 31 19:29:17 2012 Z  
Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\acrobat\_sl.exe  
ModTime: Thu Sep 24 15:40:41 2015 Z  
Executed

C:\ProgramData\dell\drivers\multiplatform\_bios\_btrfstboot\x86\_64\HAPI\dcmddev64.exe  
ModTime: Fri Sep 27 05:56:25 2013 Z  
Executed

c:\PROGRA~1\COMMON~1\mcafee\updmgr\306048~1.2\MCPUPDA~1.EXE  
ModTime: Wed Nov 4 15:54:50 2015 Z  
Executed

C:\Windows\system32\PING.EXE  
ModTime: Tue Jul 14 01:39:26 2009 Z  
Executed

C:\Program Files (x86)\WebEx\Document Suite\WbxDLInst.exe  
ModTime: Fri Sep 11 08:20:04 2015 Z  
Executed

C:\Users\Abe-Arjun Malik\Downloads\Fitbit-Uploader-For-Windows-2.1.0.9.exe  
ModTime: Sat Nov 28 20:02:00 2015 Z  
Executed

C:\Program Files\Windows Media Player\wmpnscfg.exe  
ModTime: Tue Jul 14 01:39:56 2009 Z  
Executed

C:\WINDOWS\system32\wbem\unsecapp.exe  
ModTime: Tue Jul 14 01:39:48 2009 Z  
Executed

C:\Program Files (x86)\Cisco Systems\Cisco IP Communicator\AudioTuningWizard.exe  
ModTime: Tue Feb 12 18:14:26 2013 Z  
Executed

C:\Windows\servicing\TrustedInstaller.exe  
ModTime: Sun Nov 21 03:24:03 2010 Z  
Executed

C:\Program Files\McAfee\MSC\McAPExe.exe  
ModTime: Thu Dec 3 20:15:48 2015 Z  
Executed

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\Temp\1882575568\AdobeARMHelper.exe

## SYSTEM OUTPUT

ModTime: Thu Sep 24 12:40:42 2015 Z  
Executed

C:\WINDOWS\TEMP\E3F58445-05BE-4AC6-91B5-6EB6F1A30CA8\dismhost.exe  
ModTime: Fri May 30 08:07:49 2014 Z  
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\VSCore\x64\mfehidin.exe  
ModTime: Mon Apr 18 15:58:25 2016 Z  
Executed

C:\Windows\SysWOW64\mspaint.exe  
ModTime: Tue Jul 14 01:14:26 2009 Z  
Executed

C:\Windows\system32\schtasks.exe  
ModTime: Sun Nov 21 03:23:51 2010 Z  
Executed

C:\Windows\sysWOW64\wbem\wmiprvse.exe  
ModTime: Sun Nov 21 03:24:27 2010 Z  
Executed

C:\Windows\SysWOW64\mssvp.dll  
ModTime: Wed May 4 04:32:02 2011 Z

c:\PROGRA~1\mcafee.com\agent\mcagent.exe  
ModTime: Thu Dec 3 20:15:48 2015 Z  
Executed

C:\WINDOWS\system32\oobe\oobeldr.exe  
ModTime: Tue Jul 14 01:39:26 2009 Z  
Executed

C:\Windows\system32\UI0Detect.exe  
ModTime: Tue Jul 14 01:39:48 2009 Z  
Executed

C:\Windows\TEMP\F46B7D9E-25D0-4EDB-BBB6-8D0AB9F47224\dismhost.exe  
ModTime: Sat Nov 29 16:13:49 2014 Z  
Executed

C:\Program Files (x86)\TurboTax\Deluxe 2015\32bit\TurboTax.exe  
ModTime: Wed Oct 14 12:15:09 2015 Z  
Executed

C:\ProgramData\FLEXnet\Connect\11\dwusplay.exe  
ModTime: Wed Jan 21 21:42:22 2009 Z



## SYSTEM-OUTPUT

C:\Windows\SysWOW64\reg.exe

ModTime: Tue Jul 14 01:39:29 2009 Z

Executed

C:\Windows\system32\DXPServer.exe

ModTime: Tue Jul 14 01:39:08 2009 Z

Executed

C:\Program Files (x86)\Nuance\PaperPort\ScannerWizardU.exe

ModTime: Tue Sep 21 22:57:30 2010 Z

C:\Windows\System32\acppage.dll

ModTime: Sun Nov 21 03:24:23 2010 Z

C:\Users\ABE-AR~1\AppData\Local\Temp\is-808QH.tmp\1clickdvdcopyssetup6.1.0.6.tmp

ModTime: Fri Apr 8 11:34:42 2016 Z

Executed

C:\Windows\System32\XPSSHHDR.dll

ModTime: Tue Jul 14 01:41:59 2009 Z

C:\WINDOWS\system32\calc.exe

ModTime: Tue Jul 14 01:38:57 2009 Z

C:\Windows\system32\Hpsservice.exe

ModTime: Wed Apr 25 18:02:52 2012 Z

Executed

C:\Windows\system32\net.exe

ModTime: Tue Jul 14 01:14:27 2009 Z

C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility  
Client\ManifestTool.exe

ModTime: Wed Mar 12 20:53:06 2014 Z

Executed

C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamservice.exe

ModTime: Mon Oct 5 13:48:45 2015 Z

Executed

C:\Program Files (x86)\McAfee\Common Framework\msaconfig.exe

ModTime: Tue Feb 10 20:07:59 2015 Z

Executed

C:\ProgramData\dell\drivers\multiplatform\_bios\_btrfstboot\x86\_64\HAPI\dchcfg64.exe

ModTime: Fri Sep 27 05:56:29 2013 Z

Executed

## SYSTEM OUTPUT

C:\WINDOWS\WinSxS\amd64\_microsoft-windows-ie-pdm-configuration\_31bf3856ad364e35\_11.2.9600.16428\_none\_32a601ad2b7a554f\PDMSetup.exe

ModTime: Tue Dec 29 19:21:35 2015 Z

Executed

C:\Program Files (x86)\Nuance\PaperPort\ppdebug.exe

ModTime: Tue Aug 2 21:47:52 2011 Z

C:\Windows\System32\dinotify.exe

ModTime: Tue Jul 14 01:39:06 2009 Z

Executed

C:\WINDOWS\SysWOW64\dism.exe

ModTime: Tue Jul 14 01:39:06 2009 Z

Executed

C:\Users\Abe-Arjun Malik\Downloads\KantoPlayer(2).exe

ModTime: Tue Feb 16 01:35:06 2016 Z

C:\ProgramData\FLEXnet\Connect\11\ISUSPM.exe

ModTime: Thu Oct 13 03:11:33 2011 Z

Executed

C:\Users\Nikita\Downloads\GoogleEarthSetup.exe

ModTime: Wed Jan 13 23:13:12 2016 Z

Executed

C:\Program Files (x86)\McAfee\Common Framework\x86\macompatsvc.exe

ModTime: Wed Sep 23 23:56:46 2015 Z

Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB3023221-x64.exe

ModTime: Thu Mar 10 20:44:31 2016 Z

Executed

C:\Program Files (x86)\Fitbit Connect\Fitbit Connect.exe

ModTime: Wed Oct 28 22:13:04 2015 Z

Executed

C:\WINDOWS\system32\services.exe

ModTime: Mon Apr 13 03:28:33 2015 Z

Executed

C:\Program Files (x86)\Consumer Input\Monitoring\dca-monitoring.exe

ModTime: Tue Feb 9 09:28:32 2016 Z

Executed

## SYSTEM OUTPUT

C:\Windows\System32\SystemPropertiesRemote.exe  
ModTime: Tue Jul 14 01:39:47 2009 Z

C:\Windows\TEMP\018470~1.EXE  
ModTime: Wed Oct 28 20:05:58 2015 Z  
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\VstskMgr.exe  
ModTime: Thu Jan 16 00:08:00 2014 Z  
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB3032662-x64.exe  
ModTime: Thu Mar 10 20:44:08 2016 Z  
Executed

C:\Program Files (x86)\Nuance\PaperPort\pppagevw.exe  
ModTime: Tue Aug 2 21:48:56 2011 Z

C:\Program Files (x86)\McAfee\Host Intrusion Prevention\Helper.exe  
ModTime: Thu Jun 25 01:31:02 2015 Z  
Executed

C:\Windows\system32\defrag.exe  
ModTime: Tue Jul 14 01:39:02 2009 Z  
Executed

C:\Users\ad\_dcc\_s.nchotu\AppData\Local\Temp\g2mA498.tmp\G2MInstHigh.exe  
ModTime: Tue Apr 19 20:40:39 2016 Z  
Executed

C:\Windows\Installer\MSI3DB1.tmp  
ModTime: Thu Jan 14 16:37:04 2016 Z  
Executed

c:\dac6f6cbcef6992dde8507\Setup.exe  
ModTime: Sun Jun 12 04:36:34 2011 Z  
Executed

C:\WINDOWS\SysWOW64\PstartSr.exe  
ModTime: Tue Oct 8 22:56:21 2013 Z  
Executed

C:\Windows\system32\mstsc.exe  
ModTime: Tue Oct 1 23:31:09 2013 Z

C:\Program Files (x86)\Java\jre6\bin\jqs.exe  
ModTime: Mon Apr 18 15:54:07 2016 Z  
Executed

## SYSTEM OUTPUT

C:\Users\Nikita\Downloads\download-audiograbber.exe

ModTime: Tue Jan 12 01:24:41 2016 Z

Executed

C:\Windows\SoftwareDistribution\Download\Install\vcredist\_x64.exe

ModTime: Fri Jun 3 17:31:07 2011 Z

Executed

C:\WINDOWS\SYSTEM32\TAPIUNATTEND.EXE

ModTime: Tue Jul 14 01:39:47 2009 Z

Executed

C:\Windows\System32\wiawow64.exe

ModTime: Tue Jul 14 01:39:52 2009 Z

Executed

C:\\_SMSTaskSequence\Packages\FDA000DB\jinit1319\SETUP.EXE

ModTime: Wed Dec 17 16:30:30 1997 Z

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe

ModTime: Thu Mar 20 22:49:18 2014 Z

Executed

C:\Program Files\DellTPad\Apoint.exe

ModTime: Thu Apr 16 19:14:31 2015 Z

Executed

C:\Program Files\Common Files\McAfee\CSP\mccspinstall.exe

ModTime: Thu Jan 21 07:54:14 2016 Z

Executed

C:\Program Files\McAfee\MSC\McBootSvcSet.exe

ModTime: Tue Jan 5 15:25:16 2016 Z

Executed

C:\WINDOWS\CCM\CcmRestart.exe

ModTime: Tue Apr 14 08:00:00 2015 Z

Executed

C:\WINDOWS\system32\cmd.exe

ModTime: Sun Nov 21 03:24:03 2010 Z

D:\install\MFC-9340CDW\Setup.exe

ModTime: Fri Sep 14 04:15:27 2012 Z

C:\Windows\TEMP\030505~1.EXE

ModTime: Wed Oct 28 20:05:58 2015 Z

## SYSTEM OUTPUT

Executed

C:\Users\Abe-Arjun Malik\AppData\Local\Google\Chrome\User  
Data\SwReporter\4.30.1\software\_reporter\_tool.exe

ModTime: Tue Sep 8 20:07:54 2015 Z

Executed

C:\\_SMSTaskSequence\Packages\FDA000DB\JInit13126\data1.hdr

ModTime: Tue May 16 09:50:54 2006 Z

C:\Windows\System32\timeout.exe

ModTime: Tue Jul 14 01:39:47 2009 Z

C:\Program Files (x86)\Nuance\PaperPort\ppscanmg.exe

ModTime: Tue Aug 2 21:49:14 2011 Z

C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe

ModTime: Sun Nov 21 03:24:52 2010 Z

Executed

C:\WINDOWS\SysWOW64\PING.EXE

ModTime: Tue Jul 14 01:14:28 2009 Z

Executed

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\regtliv12.exe

ModTime: Sat Apr 12 03:39:56 2014 Z

Executed

C:\Program Files\McAfee\Host Intrusion Prevention\FireTray.exe

ModTime: Thu Jun 25 01:34:26 2015 Z

Executed

C:\Windows\Installer\MSID906.tmp

ModTime: Wed Apr 13 11:28:22 2016 Z

Executed

C:\WINDOWS\Setup\Scripts\SetupComplete.cmd

ModTime: Mon Apr 18 15:26:01 2016 Z

C:\Program Files (x86)\LG Software Innovations\1Click DVD Copy  
Pro\1ClickDvdCopyPro.exe

ModTime: Thu Feb 4 21:19:14 2016 Z

Executed

C:\Users\Nikita\Downloads\filmora-bing\_setup\_full1901.exe

ModTime: Mon Apr 18 21:55:27 2016 Z

Executed

## SYSTEM OUTPUT

C:\Windows\System32\spoolsv.exe

ModTime: Sat Nov 29 16:09:44 2014 Z

Executed

C:\Windows\system32\taskhost.exe

ModTime: Sat Nov 29 16:10:16 2014 Z

Executed

C:\WINDOWS\system32\{C1D72DEE-FF54-4835-8F1C-DF56D09A95BE}.bat

ModTime: Mon Apr 18 16:25:28 2016 Z

C:\PROGRA~1\COMMON~1\McAfee\platform\McUICnt.exe

ModTime: Mon Jan 4 01:25:22 2016 Z

Executed

C:\Users\Abe-Arjun Malik\AppData\Local\Temp\cw.exe

ModTime: Mon Mar 23 19:59:13 2015 Z

C:\Program Files (x86)\McAfee\Common Framework\x86\McTray.exe

ModTime: Sat Jun 27 00:37:15 2015 Z

Executed

C:\Program Files (x86)\McAfee\Common Framework\CmdAgent.exe

ModTime: Tue Feb 10 20:07:59 2015 Z

Executed

C:\Program Files (x86)\Common Files\Intuit\Update Service v4\IntuitUpdateService.exe

ModTime: Mon Apr 27 18:43:32 2015 Z

Executed

C:\Users\AD\_DCC~1.NCH\AppData\Local\Temp\DMT\_Files\UpdateINI.exe

ModTime: Wed Nov 13 23:02:07 2013 Z

Executed

C:\PROGRA~3\McAfee\Update\Installs\pkg\_default\Download\_Files\shared\mcinst\mcinst\_cat\mcinst.exe

ModTime: Fri Nov 27 14:49:14 2015 Z

Executed

C:\WINDOWS\SysWOW64\cmd.exe

ModTime: Sun Nov 21 03:24:03 2010 Z

Executed

C:\Program Files\Common Files\System\wab32.dll

ModTime: Sat Oct 1 05:45:21 2011 Z

c:\821b926440bca534ebc99c\Setup.exe

ModTime: Fri Oct 2 09:16:10 2015 Z

## SYSTEM OUTPUT

Executed

C:\Windows\System32\igfxpph.dll  
ModTime: Thu Mar 20 15:40:19 2014 Z

C:\Windows\Explorer.EXE  
ModTime: Sat Nov 29 16:04:56 2014 Z  
Executed

C:\\_SMSTaskSequence\Packages\FDA00171\InstallDotNet4.cmd  
ModTime: Fri Jan 31 17:58:36 2014 Z

C:\WINDOWS\system32\wusa.exe  
ModTime: Sun Nov 21 03:24:08 2010 Z

C:\WINDOWS\SysWOW64\Macromed\Flash\FlashUtil32\_20\_0\_0\_235\_Plugin.exe  
ModTime: Mon Apr 18 15:45:12 2016 Z  
Executed

C:\Program Files (x86)\Cisco Systems\Cisco IP Communicator\CDP\CDPinstall.exe  
ModTime: Mon Jan 24 15:37:42 2011 Z  
Executed

C:\Program Files\Windows Sidebar\sidebar.exe  
ModTime: Sun Nov 21 03:24:51 2010 Z

C:\Program Files\Common Files\Intel Security\PEF\CORE\PEFService.exe  
ModTime: Mon Dec 14 09:33:24 2015 Z  
Executed

C:\WINDOWS\ccmsetup\cache\ccmsetup.exe  
ModTime: Thu Jun 25 22:15:00 2015 Z  
Executed

C:\Windows\System32\BWContextHandler.dll  
ModTime: Tue Jul 14 01:40:13 2009 Z

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB2972215-x64.exe  
ModTime: Thu Mar 10 21:02:48 2016 Z  
Executed

C:\\_SMSTaskSequence\Packages\FDA0022E\winzip17\_64bit.cmd  
ModTime: Thu Jul 11 18:57:58 2013 Z

D:\Firefox Setup 45.0.1.exe  
ModTime: Mon Apr 11 20:35:30 2016 Z

C:\Users\Abe-Arjun Malik\AppData\Local\Apple\Apple Software Update\SetupAdmin.exe

## SYSTEM OUTPUT

ModTime: Thu Jan 7 22:08:08 2016 Z  
Executed

C:\Program Files (x86)\GUMA62D.tmp\GoogleUpdate.exe  
ModTime: Wed Apr 20 12:59:16 2016 Z  
Executed

C:\Windows\system32\WindowsAnytimeUpgradeUI.exe  
ModTime: Tue Jul 14 01:39:52 2009 Z

C:\Windows\SoftwareDistribution\Download\Install\Windows-KB890830-x64-V5.33-delta.exe  
ModTime: Wed Feb 3 22:46:54 2016 Z  
Executed

C:\Program Files  
(x86)\McAfee\SiteAdvisor\{A80DB781-A37F-416A-8311-0413A1FD2020}\mcinst.exe  
ModTime: Mon May 4 19:41:42 2015 Z  
Executed

C:\Program Files (x86)\Nuance\PaperPort\PPLinkCfg.exe  
ModTime: Tue Aug 2 21:48:30 2011 Z

C:\Users\ABE-AR~1\AppData\Local\Temp\\_is394F.exe  
ModTime: Wed May 24 17:10:41 2006 Z  
Executed

C:\Users\Nikita\AppData\Local\Temp\GUMAED1.tmp\GoogleUpdate.exe  
ModTime: Wed Jan 13 23:14:26 2016 Z  
Executed

C:\\_SMSTaskSequence\Packages\PS10018C\FrmPkg\_UPD.exe  
ModTime: Thu Jan 16 00:08:00 2014 Z  
Executed

C:\Windows\System32\vds.exe  
ModTime: Sun Nov 21 03:23:51 2010 Z  
Executed

C:\Users\Abe-Arjun  
Malik\AppData\Local\Temp\{5D609291-3685-4AAC-8681-90B08AE8DB8A}\{E98A9C92-E767-475B-8BC6-8780A86DDC72}\BrStRgin.exe  
ModTime: Mon May 10 21:02:38 2010 Z  
Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\n1s\nchsetup.exe  
ModTime: Fri Feb 5 14:17:26 2016 Z  
Executed



## SYSTEM OUTPUT

C:\WINDOWS\System32\sdclt.exe

ModTime: Sun Nov 21 03:25:06 2010 Z

Executed

C:\WINDOWS\system32\vssvc.exe

ModTime: Sun Nov 21 03:23:55 2010 Z

Executed

C:\Windows\SysWOW64\schtasks.exe

ModTime: Sun Nov 21 03:23:51 2010 Z

Executed

C:\Program Files\iPod\bin\iPodService.exe

ModTime: Fri Dec 18 03:12:34 2015 Z

Executed

C:\\_SMSTaskSequence\Packages\PS1002EF\osd\_flash20inst\_npapi.cmd

ModTime: Wed Dec 16 19:29:11 2015 Z

C:\WINDOWS\SysWOW64\netsh.exe

ModTime: Tue Jul 14 01:14:27 2009 Z

Executed

C:\Program Files (x86)\Windows Media Player\wmpshare.exe

ModTime: Wed Apr 29 18:06:48 2015 Z

Executed

C:\Program Files (x86)\Google\Update\1.3.29.1\GoogleCrashHandler.exe

ModTime: Sun Dec 6 01:15:24 2015 Z

Executed

C:\Windows\system32\DrvInst.exe

ModTime: Tue Jul 14 01:39:07 2009 Z

Executed

C:\Program Files\Common Files\McAfee\CSP\1.8.267.0\McCSPServiceHost.exe

ModTime: Tue Feb 23 10:43:04 2016 Z

Executed

C:\Program Files (x86)\Common Files\Apple\Apple Application Support\APSDaemon.exe

ModTime: Fri May 15 20:26:48 2015 Z

Executed

C:\Program Files (x86)\webex\Productivity Tools\ptonecli64.dll

ModTime: Mon Oct 12 06:06:12 2015 Z

C:\Program Files\McAfee\MSC\Partner\SAInstallManager\McPartnerSAInstallManager.exe

## SYSTEM OUTPUT

ModTime: Tue Jul 7 06:44:45 2015 Z  
Executed

C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe  
ModTime: Tue Jul 14 01:39:20 2009 Z

C:\Program Files (x86)\Microsoft Lync\communicator.exe  
ModTime: Thu Nov 12 22:00:18 2015 Z  
Executed

C:\Windows\System32\fsquirt.exe  
ModTime: Sun Nov 21 03:23:47 2010 Z  
Executed

C:\Windows\SYSTEM32\WISPTIS.EXE  
ModTime: Sun Nov 21 03:25:10 2010 Z  
Executed

C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\aspnet\_regiis.exe  
ModTime: Thu Mar 18 21:23:04 2010 Z  
Executed

C:\WINDOWS\Installer\MSIE7D4.tmp  
ModTime: Tue Apr 19 20:40:56 2016 Z  
Executed

C:\Program Files (x86)\Nuance\PDF Create 8\bin\GPDFDirect.exe  
ModTime: Mon May 7 21:10:56 2012 Z

C:\Users\Nikita\Downloads\filmora-bing\_setup\_full1901 (1).exe  
ModTime: Mon Apr 18 21:55:28 2016 Z

C:\progra~2\java\jre-1.6.38\zipper.exe  
ModTime: Wed Nov 14 09:18:29 2012 Z  
Executed

C:\Program Files\Common Files\ActivIdentity\ac.sharedstore.exe  
ModTime: Wed Jun 3 21:38:36 2009 Z  
Executed

C:\DMTFiles\usmt\5\X64\loadstate.exe  
ModTime: Thu Jul 26 01:12:12 2012 Z  
Executed

C:\Windows\TEMP\CR\_161D1.tmp\setup.exe  
ModTime: Fri Feb 5 00:21:11 2016 Z  
Executed

## SYSTEM OUTPUT

C:\Program Files\Common Files\McAfee\Platform\mcaicnt.exe

ModTime: Tue Nov 3 01:06:06 2015 Z

Executed

C:\ProgramData\webex\WebEx\1525\WbxDLInst.exe

ModTime: Fri Sep 11 08:20:04 2015 Z

Executed

C:\WINDOWS\system32\mfevtps.exe

ModTime: Mon Apr 18 15:58:25 2016 Z

Executed

C:\Windows\SysWOW64\runonce.exe

ModTime: Sun Nov 21 03:23:53 2010 Z

Executed

C:\Windows\System32\extrac32.exe

ModTime: Tue Jul 14 01:14:20 2009 Z

C:\WINDOWS\TEMP\IE130DF.tmp\IE11-SUPPORT\IEXPLORE.EXE

ModTime: Mon Oct 14 22:48:14 2013 Z

Executed

C:\Program Files\Common Files\McAfee\CSP\1.8.259.0\McCSPServiceHost.exe

ModTime: Thu Jan 21 07:51:26 2016 Z

Executed

C:\Windows\System32\tcmsetup.exe

ModTime: Tue Jul 14 01:39:47 2009 Z

C:\WINDOWS\TEMP\{5233B566-C0A7-499B-B831-47304F434D11}\InstallFlashPlayer.exe

ModTime: Wed Apr 20 14:55:56 2016 Z

Executed

C:\Windows\TEMP\D352F96C-E6DC-4D56-8D40-1D27C479AA83\dismhost.exe

ModTime: Sat Nov 29 16:13:49 2014 Z

Executed

C:\Windows\Installer\{91120000-002F-0000-0000-00000000FF1CE}\xlicons.exe

ModTime: Wed Dec 16 22:29:46 2015 Z

C:\Program Files (x86)\Consumer Input\Monitoring\uninstall.exe

ModTime: Tue Feb 9 09:29:36 2016 Z

C:\Windows\TEMP\1D1482F3-B6B7-42D7-B65A-EA2762784F50\dismhost.exe

ModTime: Sat Nov 29 16:13:49 2014 Z

Executed

## SYSTEM OUTPUT

C:\Windows\System32\ntshrui.dll

ModTime: Sat Nov 29 16:06:06 2014 Z

C:\Windows\system32\makecab.exe

ModTime: Tue Jul 14 01:39:16 2009 Z

Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB2978125-x64.exe

ModTime: Thu Mar 10 21:00:23 2016 Z

Executed

C:\Windows\fveupdate.exe

ModTime: Tue Jul 14 01:39:10 2009 Z

Executed

C:\Users\Nikita\Downloads\CardReader\_Realtek\_Win7\_64\_VER62920027040\setup.exe

ModTime: Mon Jan 28 21:19:28 2013 Z

C:\Windows\Sysnative\regsvr32.exe

ModTime: Tue Jul 14 01:39:29 2009 Z

C:\Program Files\Common Files\McAfee\CSP\mccspuninstall.exe

ModTime: Wed Dec 2 15:05:14 2015 Z

Executed

C:\Windows\system32\mspaint.exe

ModTime: Tue Jul 14 01:39:24 2009 Z

C:\WINDOWS\Installer\MSICD0D.tmp

ModTime: Mon Apr 18 15:58:26 2016 Z

Executed

C:\Windows\system32\taskmgr.exe

ModTime: Sun Nov 21 03:24:24 2010 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\GUM7718.tmp\ConsumerInputUpdate.exe

ModTime: Sat Feb 20 01:46:11 2016 Z

Executed

C:\\_SMSTaskSequence\Packages\FDA000DB\jInit13113\SETUP.EXE

ModTime: Wed Dec 17 15:30:30 1997 Z

C:\Program Files (x86)\Nuance\PaperPort\IndexSearch.exe

ModTime: Tue Aug 2 21:45:06 2011 Z

Executed

C:\Windows\system32\icacls.exe

## SYSTEM OUTPUT

ModTime: Tue Jul 14 01:14:21 2009 Z

C:\WINDOWS\TEMP\vccredist\_x64\_2005.exe

ModTime: Thu Jun 14 15:05:20 2012 Z

Executed

C:\Windows\System32\GWX\GWXUX.exe

ModTime: Tue Dec 8 19:06:56 2015 Z

Executed

C:\Program Files (x86)\Common Files\Adobe\Calibration\Adobe Gamma.cpl

ModTime: Tue Aug 6 18:41:33 2002 Z

C:\Program Files (x86)\Brother\Brmfl12d\BrStDvPt.exe

ModTime: Fri Aug 26 21:03:30 2011 Z

Executed

C:\Program Files (x86)\Common Files\Intuit\Update Service v4\IntuitUpdater.exe

ModTime: Mon Apr 27 18:43:32 2015 Z

Executed

C:\Program Files\McAfee.com\Agent\mcagent.exe

ModTime: Thu Dec 3 20:15:48 2015 Z

Executed

C:\\_SMSTaskSequence\Packages\PS100169\DAT-Grab.bat

ModTime: Mon Feb 24 20:18:23 2014 Z

C:\Windows\system32\CompatTelRunner.exe

ModTime: Mon Apr 4 18:14:06 2016 Z

Executed

C:\Users\Nikita\AppData\Local\Temp\smb4630\_15724.exe

ModTime: Sat Apr 2 17:08:00 2016 Z

Executed

C:\Windows\system32\sc.exe

ModTime: Tue Jul 14 01:39:35 2009 Z

Executed

C:\\_SMSTaskSequence\Packages\PS1002F3\HF1059145\McAfeeHIP\_ClientHotfix6\_1059145.exe

ModTime: Wed Sep 16 20:04:00 2015 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\DLG\requirements\compete\_precheck\_112114233405.exe

ModTime: Sat Feb 20 01:45:30 2016 Z

Executed

## SYSTEM OUTPUT

C:\Program Files (x86)\Malwarebytes Anti-Malware\mbam.exe

ModTime: Mon Oct 5 13:48:33 2015 Z

Executed

C:\Users\Nikita\AppData\Local\Temp\Rar\$EXa0.462\agmp3plugin-pro.exe

ModTime: Fri Feb 28 15:06:26 2014 Z

Executed

C:\Windows\system32\w32tm.exe

ModTime: Tue Jul 14 01:39:50 2009 Z

Executed

C:\Program Files\Common Files\McAfee\SystemCore\EntVUtil.EXE

ModTime: Mon Apr 18 15:58:25 2016 Z

Executed

C:\Program Files\Common Files\Intel Security\PEF\Installer\InstallPEF.exe

ModTime: Mon Dec 14 17:06:50 2015 Z

Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB3037578-x64.exe

ModTime: Thu Mar 10 20:45:30 2016 Z

Executed

C:\WINDOWS\WinSxS\x86\_microsoft-windows-ie-pdm-configuration\_31bf3856ad364e35\_11.2.9600.16428\_none\_d6876629731ce419\PDMSSetup.exe

ModTime: Tue Dec 29 19:21:35 2015 Z

Executed

C:\Users\Abe-Arjun Malik\Downloads\KantoPlayer.exe

ModTime: Fri Jan 8 19:09:10 2016 Z

Executed

C:\Program Files (x86)\Microsoft Lync\UcMapi.exe

ModTime: Wed Sep 25 17:01:37 2013 Z

Executed

C:\\_SMSTaskSequence\Packages\FDA00184\reg\_w7.exe

ModTime: Mon Apr 14 00:12:32 2008 Z

Executed

c:\dc37314ae06ad4c7a127b2209f\Setup.exe

ModTime: Thu Feb 5 09:15:53 2015 Z

Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB3098778-x64.exe

ModTime: Thu Mar 10 20:17:09 2016 Z

## SYSTEM OUTPUT

Executed

C:\Program Files (x86)\WIDI 4.4 Pro\Widi.exe  
ModTime: Thu Dec 10 10:51:06 2015 Z  
Executed

C:\WINDOWS\system32\taskeng.exe  
ModTime: Sun Nov 21 03:24:27 2010 Z  
Executed

C:\Windows\System32\appwiz.cpl  
ModTime: Sun Nov 21 03:24:00 2010 Z

C:\\_SMSTaskSequence\Packages\FDA0007A\IE\_tabs\_off.cmd  
ModTime: Thu Nov 10 14:13:58 2011 Z

C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe  
ModTime: Thu Mar 18 18:27:13 2010 Z  
Executed

C:\dae0984bf92096849f7d22\Setup.exe  
ModTime: Thu Mar 18 20:16:28 2010 Z  
Executed

C:\WINDOWS\Installer\MSICAE4.tmp  
ModTime: Mon Apr 18 15:58:25 2016 Z  
Executed

D:\Prerequisites\Netfx40TestApplication.exe  
ModTime: Mon Oct 19 18:27:11 2015 Z

C:\Program Files (x86)\McAfee\VirusScan Enterprise\mfeann.exe  
ModTime: Thu Jan 16 00:08:00 2014 Z  
Executed

C:\Windows\twain\_32\wiatwain.ds  
ModTime: Tue Jul 14 00:14:41 2009 Z

C:\Windows\system32\SndVol.exe  
ModTime: Sun Nov 21 03:23:53 2010 Z  
Executed

C:\Windows\WinSxS\amd64\_microsoft-windows-gwx-uninstall\_31bf3856ad364e35\_6.1.7601.19162\_none\_0b203995123a851f\GWXGC.exe  
ModTime: Sat Dec 5 14:08:28 2015 Z  
Executed

C:\WINDOWS\SysWOW64\wusa.exe

## SYSTEM OUTPUT

ModTime: Sun Nov 21 03:24:08 2010 Z  
Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\is-J73JI.tmp\KantoPlayer.tmp  
ModTime: Fri Jan 8 19:10:03 2016 Z  
Executed

C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleUpdate.exe  
ModTime: Thu Feb 4 14:13:21 2016 Z

C:\Users\ABE-AR~1\AppData\Local\Temp\{436E3108-9859-4A4F-B647-72ED12B93A5C}\ISBEW64.exe  
ModTime: Tue Feb 2 00:17:27 2016 Z  
Executed

C:\Windows\System32\TSWbPrxy.exe  
ModTime: Thu Dec 11 17:47:17 2014 Z

C:\WINDOWS\system32\RAServer.exe  
ModTime: Tue Jul 14 01:39:28 2009 Z  
Executed

C:\Windows\TEMP\027028~1.EXE  
ModTime: Fri Nov 27 14:49:14 2015 Z  
Executed

C:\Windows\system32\StikyNot.exe  
ModTime: Tue Jul 14 01:39:46 2009 Z

C:\Program Files (x86)\Brother\Firmware\Pack.exe  
ModTime: Tue Oct 9 15:27:56 2012 Z  
Executed

C:\Windows\System32\wpccpl.dll  
ModTime: Sun Nov 21 03:24:36 2010 Z

C:\Windows\system32\notepad.exe  
ModTime: Thu Jul 9 17:57:57 2015 Z

C:\ProgramData\webex\WebEx\1524\WbxDLInst.exe  
ModTime: Fri Sep 11 08:20:04 2015 Z  
Executed

C:\Windows\System32\tasklist.exe  
ModTime: Tue Jul 14 01:39:47 2009 Z

C:\Windows\Temp\nswB012.tmp\FilestoInstall\PEFHelper.exe  
ModTime: Mon Dec 14 09:33:24 2015 Z



## SYSTEM OUTPUT

Executed

C:\Program Files (x86)\Fitbit Connect\FitbitConnectService.exe  
ModTime: Wed Oct 28 22:13:04 2015 Z  
Executed

C:\\_SMSTaskSequence\Packages\PS10001F\connect.bat  
ModTime: Tue Jul 23 18:47:17 2013 Z

C:\WINDOWS\TEMP\{8D59EA37-C399-4770-85AB-352ACE11D6AA}\ISBEW64.exe  
ModTime: Mon Aug 22 05:05:39 2011 Z  
Executed

C:\Program Files (x86)\McAfee\Host Intrusion Prevention\vscore\x64\mfehidin.exe  
ModTime: Mon Jun 15 17:22:30 2015 Z  
Executed

C:\PROGRA~1\mcafee.com\agent\McUpdate.exe  
ModTime: Thu Dec 3 20:15:56 2015 Z  
Executed

C:\WINDOWS\SysWOW64\atashost.exe  
ModTime: Fri Sep 11 08:19:50 2015 Z  
Executed

C:\Windows\Installer\{91120000-002F-0000-0000-0000000FF1CE}\wordicon.exe  
ModTime: Wed Dec 16 22:29:46 2015 Z

C:\WINDOWS\system32\lodctr.exe  
ModTime: Tue Jul 14 01:39:15 2009 Z  
Executed

C:\Windows\system32\at.exe  
ModTime: Tue Jul 14 01:14:12 2009 Z

C:\Program Files (x86)\Google\Chrome\Application\48.0.2564.116\Installer\setup.exe  
ModTime: Fri Feb 19 22:18:57 2016 Z  
Executed

C:\WINDOWS\WinSxS\x86\_microsoft-windows-i..eoptionalcomponents\_31bf3856ad364e35\_11.2.9600.16428\_none\_87f259ebb3f177fa\ConfigureIEOptionalComponents.exe  
ModTime: Tue Dec 29 19:21:35 2015 Z  
Executed

C:\\_SMSTaskSequence\Packages\FDA0004E\cac1s.exe  
ModTime: Mon Apr 14 09:42:14 2008 Z  
Executed

## SYSTEM OUTPUT

C:\Program Files  
(x86)\McAfee\SiteAdvisor\{13380103-812A-4867-ADF4-405B79DA76C1}\saInst.exe  
ModTime: Thu Feb 11 21:32:56 2016 Z  
Executed

C:\ProgramData\FLEXnet\Connect\11\issch.exe  
ModTime: Tue May 5 21:06:07 2009 Z

C:\Program Files\McAfee\Host Intrusion Prevention\FireSvc.exe  
ModTime: Thu Jun 25 01:34:18 2015 Z  
Executed

C:\Program Files\McAfee\Host Intrusion Prevention\Helper.exe  
ModTime: Thu Jun 25 01:34:08 2015 Z  
Executed

C:\Users\Abe-Arjun Malik\Downloads\1clickdvdcopyprosetup5.1.0.6.exe  
ModTime: Sun Mar 27 20:32:36 2016 Z  
Executed

C:\WINDOWS\CCM\OSDSetupWindows.exe  
ModTime: Tue Apr 14 08:00:00 2015 Z  
Executed

C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerPlugin\_20\_0\_0\_286.exe  
ModTime: Tue Jan 19 21:17:59 2016 Z  
Executed

C:\PROGRA~1\COMMON~1\McAfee\Platform\MSM\McSmtFwk.exe  
ModTime: Tue Nov 3 02:18:57 2015 Z  
Executed

C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleUpdateBroker.exe  
ModTime: Thu Feb 4 14:13:21 2016 Z

C:\Windows\system32\AitStatic.exe  
ModTime: Wed Jun 3 20:16:59 2015 Z  
Executed

c:\PROGRA~2\mcafee\SITEAD~1\mcsacore.exe  
ModTime: Tue Dec 29 20:55:58 2015 Z  
Executed

C:\WINDOWS\TEMP\2E44F53D-B930-40D5-B151-1C2641F2AA4D\dismhost.exe  
ModTime: Fri May 30 08:07:49 2014 Z  
Executed

C:\Windows\Sysnative\reg.exe

## SYSTEM OUTPUT

ModTime: Tue Jul 14 01:39:29 2009 Z

C:\Program Files\Common Files\Microsoft Shared\OFFICE14\MSOXEVDLL

ModTime: Mon Mar 1 09:18:07 2010 Z

D:\fscommand\en\_MflAll6.exe

ModTime: Tue Nov 14 16:00:00 2006 Z

C:\Windows\system32\atbroker.exe

ModTime: Tue Jul 14 01:38:55 2009 Z

Executed

C:\Program Files (x86)\Nuance\PaperPort\PPMV.exe

ModTime: Tue Aug 9 22:48:14 2011 Z

C:\Windows\SoftwareDistribution\Download\Install\msxml4-KB2758694-enu.exe

ModTime: Thu Dec 20 00:24:12 2012 Z

Executed

C:\Users\Nikita\Downloads\SmileboxInstaller.exe

ModTime: Sat Apr 2 17:06:44 2016 Z

Executed

C:\WINDOWS\system32\gpscript.exe

ModTime: Tue Jul 14 01:39:11 2009 Z

Executed

C:\Program Files (x86)\McAfee\SiteAdvisor\saUI.exe

ModTime: Wed Dec 2 15:39:31 2015 Z

Executed

C:\Program Files (x86)\Cisco Systems\VPN Client\SetMTU.exe

ModTime: Fri Mar 4 16:45:35 2011 Z

Executed

C:\Program Files

(x86)\McAfee\SiteAdvisor\{7858331B-FE1D-4ACA-AEC9-F28B9E16A0C4}\mcinst.exe

ModTime: Mon May 4 20:41:41 2015 Z

Executed

C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\ServiceModelReg.exe

ModTime: Thu Mar 18 18:27:13 2010 Z

Executed

C:\WINDOWS\Installer\MSIFC6F.tmp

ModTime: Mon Apr 18 15:54:16 2016 Z

Executed

## SYSTEM OUTPUT

C:\Program Files (x86)\Audiograbber\audiograbber.exe

ModTime: Mon Feb 9 03:48:51 2004 Z

Executed

C:\Windows\system32\runonce.exe

ModTime: Sun Nov 21 03:24:27 2010 Z

Executed

C:\WINDOWS\system32\unlodctr.exe

ModTime: Tue Jul 14 01:39:48 2009 Z

Executed

C:\Users\Abe-Arjun

Malik\AppData\Local\Temp\{5D609291-3685-4AAC-8681-90B08AE8DB8A}\{E98A9C92-E767-475B-8BC6-8780A86DDC72}\BrLogRx64.exe

ModTime: Fri Feb 27 21:37:55 2009 Z

Executed

C:\Users\Nikita\AppData\Roaming\Smilebox\SmileboxUpdater.exe

ModTime: Tue Mar 1 06:39:45 2016 Z

Executed

C:\WINDOWS\system32\sc.exe

ModTime: Tue Jul 14 01:39:35 2009 Z

Executed

C:\Windows\system32\CScript.exe

ModTime: Sat Nov 29 15:57:38 2014 Z

C:\Users\Abe-Arjun Malik\Downloads\vimtag\_setup.exe

ModTime: Sun Mar 27 02:09:19 2016 Z

Executed

C:\Windows\system32\mcbuilder.exe

ModTime: Sun Nov 21 03:24:26 2010 Z

Executed

C:\Program Files (x86)\Common Files\Apple\Mobile Device

Support\AppleMobileDeviceHelper.exe

ModTime: Fri May 29 23:05:26 2015 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\{5D609291-3685-4AAC-8681-90B08AE8DB8A}\{E98A9C92-E767-475B-8BC6-8780A86DDC72}\BrLogRx.exe

ModTime: Fri Feb 27 21:38:09 2009 Z

Executed

c:\d88ce79680cc3b4427\Setup.exe

## SYSTEM OUTPUT

ModTime: Wed Jul 15 05:42:41 2015 Z  
Executed

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE14\msoshext.dll  
ModTime: Wed Jun 26 01:19:36 2013 Z

C:\WINDOWS\Installer\MSI21A6.tmp  
ModTime: Tue Apr 19 20:41:11 2016 Z  
Executed

C:\Windows\TEMP\007693~1.EXE  
ModTime: Mon May 4 20:41:41 2015 Z  
Executed

C:\Users\Nikita\AppData\Local\Microsoft\Windows\Burn\Burn\Audio\_Realtek\_Win7\_64\_VER6  
017213\Setup.exe  
ModTime: Mon Nov 14 20:24:00 2005 Z

C:\Users\Nikita\AppData\Local\Temp\Rar\$EXa0.293\agsetup183pro.exe  
ModTime: Sat Aug 30 10:38:20 2014 Z  
Executed

C:\Program Files (x86)\Brother\Firmware\res\BrPdr\BrPdrMai.exe  
ModTime: Wed Jun 29 22:58:15 2011 Z  
Executed

C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe  
ModTime: Thu Jan 7 22:17:26 2016 Z  
Executed

C:\WINDOWS\system32\SnippingTool.exe  
ModTime: Tue Jul 14 01:39:41 2009 Z

C:\Windows\SysWOW64\tquery.dll  
ModTime: Sat Nov 29 16:05:18 2014 Z

C:\Users\ABE-AR~1\AppData\Local\Temp\is-CEIB0.tmp\DVD43\_Plugin\_Setup\_1.0.0.6.tmp  
ModTime: Sun Mar 27 20:36:16 2016 Z  
Executed

C:\Windows\sysnative\sc.exe  
ModTime: Tue Jul 14 01:39:35 2009 Z

C:\WINDOWS\system32\{86F549EB-A66B-4D6C-958D-CDDD66410751}.bat  
ModTime: Mon Apr 18 16:25:28 2016 Z

C:\Windows\system32\fxssvc.exe  
ModTime: Sun Nov 21 03:25:14 2010 Z

## SYSTEM OUTPUT

Executed

C:\Windows\System32\wmpshell.dll

ModTime: Sun Nov 21 03:24:52 2010 Z

C:\Windows\Temp\nshD2F.tmp\FilestoInstall\PEFHelper.exe

ModTime: Mon Dec 14 09:33:24 2015 Z

Executed

C:\PROGRA~2\WebEx\PRODUC~1\ptWbxONI.exe

ModTime: Mon Oct 12 06:06:12 2015 Z

Executed

C:\Windows\Temp\{61667728-A947-4C81-B55B-BC0DB504A47B}\Disk1\data1.hdr

ModTime: Mon Apr 18 16:02:56 2016 Z

C:\Users\Abe-Arjun

Malik\AppData\Local\Adobe\4C8BAB87-784D-4819-8C69-19F593639E7B\gtcheck.exe

ModTime: Sat Feb 6 20:05:37 2016 Z

Executed

C:\Windows\System32\docprop.dll

ModTime: Tue Jul 14 01:40:32 2009 Z

c:\9c47e7d1ab4b0e91c3077b8e5c\install.exe

ModTime: Sat Dec 12 06:11:00 2015 Z

Executed

C:\Program Files

(x86)\McAfee\SiteAdvisor\{13380103-812A-4867-ADF4-405B79DA76C1}\mcinst.exe

ModTime: Mon May 4 20:41:41 2015 Z

Executed

C:\Users\Nikita\Downloads\video-editor-bing\_setup\_full1661.exe

ModTime: Sat Apr 2 17:47:29 2016 Z

Executed

C:\\_SMSTaskSequence\OSD\PS10018F\ccmsetup.exe

ModTime: Thu Jun 25 22:15:00 2015 Z

Executed

D:\paperport\PPImgPrinter\System64\setup.exe

ModTime: Mon Jun 18 06:43:50 2012 Z

C:\Program Files (x86)\McAfee\SiteAdvisor\Download\s26s.11.exe

ModTime: Sun Mar 6 17:56:16 2016 Z

Executed

## SYSTEM OUTPUT

C:\WINDOWS\Installer\MSIAFD1.tmp  
ModTime: Wed Apr 20 14:58:37 2016 Z  
Executed

C:\Program Files\Common Files\Intel Security\PEF\CORE\PEFUpdater.exe  
ModTime: Mon Dec 14 09:33:24 2015 Z  
Executed

C:\Windows\system32\wbem\WmiApSrv.exe  
ModTime: Tue Jul 14 01:39:55 2009 Z  
Executed

c:\632d0829f292c3d51ff3c4ef\Setup.exe  
ModTime: Fri Sep 5 16:26:44 2014 Z  
Executed

C:\Windows\SysWOW64\taskkill.exe  
ModTime: Tue Jul 14 01:14:42 2009 Z  
Executed

C:\WINDOWS\system32\netsh.exe  
ModTime: Tue Jul 14 01:14:27 2009 Z  
Executed

C:\WINDOWS\TEMP\{138211E2-283F-4ACA-A8B3-C76F016DDF90}\InstallFlashPlayer.exe  
ModTime: Wed Apr 20 14:56:09 2016 Z  
Executed

C:\Windows\SysWOW64\mshta.exe  
ModTime: Mon Dec 1 14:07:38 2014 Z  
Executed

C:\Users\Abe-Arjun Malik\AppData\Local\Temp\compete.exe  
ModTime: Sat Feb 20 01:46:04 2016 Z

C:\progra~2\java\jre-1.6.38\bin\unpack200.exe  
ModTime: Mon Apr 18 15:54:25 2016 Z  
Executed

C:\Program Files (x86)\WebEx\Document Suite\ATKCall.exe  
ModTime: Fri Sep 11 08:19:50 2015 Z  
Executed

C:\Users\Abe-Arjun Malik\AppData\Local\Temp\ose00000.exe  
ModTime: Sat Oct 28 05:28:25 2006 Z

C:\Windows\system32\sppsvc.exe  
ModTime: Sun Nov 21 03:23:56 2010 Z

## SYSTEM OUTPUT

Executed

C:\Program Files (x86)\McAfee\Common Framework\frminst.exe

ModTime: Tue Feb 10 20:07:59 2015 Z

Executed

C:\WINDOWS\system32\wbem\WMIADAP.EXE

ModTime: Tue Jul 14 01:39:55 2009 Z

Executed

C:\Windows\System32\fdprint.dll

ModTime: Tue Jul 14 01:40:52 2009 Z

C:\Program Files (x86)\GUM8E77.tmp\GoogleUpdate.exe

ModTime: Thu Feb 4 14:13:21 2016 Z

Executed

C:\Program Files\ActivIdentity\ActivClient\accrdsb.exe

ModTime: Wed Jun 3 21:36:22 2009 Z

Executed

C:\Windows\Installer\MSIDFEE.tmp

ModTime: Tue Feb 2 00:19:55 2016 Z

Executed

C:\Windows\system32\GWX\GWXDetector.exe

ModTime: Tue Dec 8 19:06:56 2015 Z

Executed

C:\PROGRA~2\WebEx\PRODUC~1\ptSrv.exe

ModTime: Mon Oct 12 06:06:12 2015 Z

Executed

C:\WINDOWS\CCM\RemCtrl\SccmRdpSystem.exe

ModTime: Tue Apr 14 08:00:00 2015 Z

Executed

C:\Program Files (x86)\Google\Chrome\Application\47.0.2526.106\Installer\chromstp.exe

ModTime: Wed Dec 16 22:05:57 2015 Z

Executed

C:\Program Files\Realtek\Audio\HDA\RtkNGUI64.exe

ModTime: Thu Apr 16 19:14:29 2015 Z

Executed

C:\Windows\System32\tracert.exe

ModTime: Mon May 25 18:18:45 2015 Z



## SYSTEM OUTPUT

C:\Program Files (x86)\Brother\Brmfl12d\Brolink\Brolink0.exe  
ModTime: Fri Oct 22 07:41:44 2004 Z  
Executed

C:\Program Files (x86)\Microsoft Office\Office14\BCSSync.exe  
ModTime: Mon Nov 5 19:27:46 2012 Z  
Executed

C:\Windows\SysWOW64\Macromed\Flash\FlashUtil32\_20\_0\_0\_286\_Plugin.exe  
ModTime: Tue Jan 19 21:17:59 2016 Z  
Executed

C:\Windows\Installer\{91120000-002F-0000-0000-0000000FF1CE}\pptico.exe  
ModTime: Wed Dec 16 22:29:46 2015 Z

C:\Users\ABE-AR~1\AppData\Local\Temp\is-54C4Q.tmp\1clickdvdcopyprosetup5.1.0.6.tmp  
ModTime: Fri Apr 8 11:32:03 2016 Z  
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\shext.dll  
ModTime: Thu Jan 16 00:08:00 2014 Z

C:\Windows\system32\compattel\DiagTrackRunner.exe  
ModTime: Wed Jun 3 20:17:05 2015 Z  
Executed

C:\Program Files  
(x86)\Google\Update\Install\{2533FAE5-E51B-4CD0-A76A-F51FF6538401}\GoogleEarth-Win-B  
undle-7.1.5.1557.exe  
ModTime: Wed Jan 13 23:14:50 2016 Z  
Executed

C:\Program Files\McAfee\MSC\OOBE\mcocrollback.exe  
ModTime: Fri Sep 25 20:21:10 2015 Z  
Executed

C:\WINDOWS\SysWOW64\Macromed\Flash\FlashUtil32\_20\_0\_0\_228\_ActiveX.exe  
ModTime: Mon Apr 18 15:45:05 2016 Z  
Executed

C:\Program Files (x86)\Nuance\PaperPort\ppocrmg.exe  
ModTime: Tue Aug 2 21:48:48 2011 Z

C:\Users\AD\_DCC~1.NCH\AppData\Local\Temp\DMT\_Files\USMT\USMTPercentScan.exe  
ModTime: Thu Dec 12 21:10:36 2013 Z  
Executed

C:\Program Files (x86)\Nuance\PaperPort\ppprint.exe

## SYSTEM OUTPUT

ModTime: Tue Aug 2 21:49:02 2011 Z

C:\Windows\Installer\{90140000-0011-0000-0000-0000000FF1CE}\xlicons.exe

ModTime: Wed Dec 30 12:57:23 2015 Z

C:\WINDOWS\system32\igfxHK.exe

ModTime: Thu Apr 16 19:14:55 2015 Z

Executed

C:\Windows\System32\usercpl.dll

ModTime: Sun Nov 21 03:24:03 2010 Z

C:\Program Files (x86)\Audiograbber\Uninstall.exe

ModTime: Tue Jan 12 01:30:30 2016 Z

C:\WINDOWS\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe

ModTime: Sun Nov 21 03:24:52 2010 Z

Executed

C:\WINDOWS\Installer\MSI1FF0.tmp

ModTime: Tue Apr 19 20:41:10 2016 Z

Executed

C:\Program Files (x86)\Windows Media Player\wmplayer.exe

ModTime: Wed Apr 29 18:06:48 2015 Z

Executed

C:\Windows\Installer\{90140000-001A-0000-0000-0000000FF1CE}\outicon.exe

ModTime: Wed Dec 16 22:29:05 2015 Z

C:\ProgramData\webex\WebEx\1530\WbxDLInst.exe

ModTime: Fri Sep 11 08:20:04 2015 Z

Executed

C:\Windows\System32\dskquoui.dll

ModTime: Sun Nov 21 03:24:26 2010 Z

C:\WINDOWS\SysWOW64\find.exe

ModTime: Tue Jul 14 01:14:20 2009 Z

Executed

C:\Program Files (x86)\LG Software Innovations\1Click DVD Copy 6\1ClickDvdCopy.exe

ModTime: Thu Feb 4 21:19:12 2016 Z

Executed

C:\Program Files (x86)\McAfee\SiteAdvisor\Download\sbnc.u.exe

ModTime: Thu Jan 28 00:30:54 2016 Z

Executed

## SYSTEM OUTPUT

C:\WINDOWS\UDI\IsTouchEnabled.exe

ModTime: Fri Jun 7 16:00:34 2013 Z

Executed

C:\Program Files\Microsoft Office\Office14\ONFILTER.DLL

ModTime: Fri Jun 28 03:09:56 2013 Z

C:\WINDOWS\system32\unregmp2.exe

ModTime: Tue Jul 14 01:39:48 2009 Z

Executed

C:\Program Files (x86)\Google\Update\1.3.29.1\GoogleCrashHandler64.exe

ModTime: Sun Dec 6 01:15:24 2015 Z

Executed

C:\WINDOWS\Installer\MSICF6F.tmp

ModTime: Mon Apr 18 15:58:26 2016 Z

Executed

C:\Users\Nikita\AppData\Roaming\Smilebox\SmileboxStarter.exe

ModTime: Tue Mar 1 10:39:46 2016 Z

Executed

C:\WINDOWS\system32\lsim.exe

ModTime: Sun Nov 21 03:23:53 2010 Z

Executed

C:\Windows\TEMP\017052~1.EXE

ModTime: Wed Oct 28 20:05:58 2015 Z

Executed

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe

ModTime: Thu Sep 24 15:40:41 2015 Z

Executed

C:\Windows\system32\calc.exe

ModTime: Tue Jul 14 01:38:57 2009 Z

D:\GlobalSubmitReview\GSReview2014\Sleep\_xp.exe

ModTime: Fri Aug 15 00:59:00 2003 Z

C:\WINDOWS\Installer\MSICF81.tmp

ModTime: Mon Apr 18 15:58:26 2016 Z

Executed

C:\Program Files (x86)\Kanto Player\unins000.exe

ModTime: Tue Feb 16 01:35:16 2016 Z

## SYSTEM OUTPUT

Executed

C:\Windows\system32\SearchIndexer.exe

ModTime: Sat Nov 29 16:05:18 2014 Z

Executed

C:\Windows\SysWOW64\mf.dll

ModTime: Tue Dec 8 21:53:47 2015 Z

C:\Windows\System32\tzutil.exe

ModTime: Sun Nov 21 03:23:52 2010 Z

C:\Windows\SysWOW64\networkexplorer.dll

ModTime: Sun Nov 21 03:24:15 2010 Z

C:\Program Files (x86)\Mozilla Firefox\maintenanceservice\_installer.exe

ModTime: Wed Mar 16 01:47:33 2016 Z

Executed

C:\\_SMSTaskSequence\Packages\FDA000DB\JInit13126\Setup.exe

ModTime: Wed Sep 5 10:23:24 2001 Z

Executed

C:\Program Files (x86)\Common Files\Apple\Mobile Device Support\ATH.exe

ModTime: Wed Oct 7 16:45:37 2015 Z

Executed

C:\PROGRA~3\WebEx\WebEx\T30\_TC\ATSHELL.EXE

ModTime: Sun Jan 31 18:05:30 2016 Z

Executed

C:\Program Files\Realtek\Audio\HDA\RtkAudioService64.exe

ModTime: Thu Apr 16 19:14:29 2015 Z

Executed

D:\GlobalSubmitReview\GSReview2014\SetACL.exe

ModTime: Wed Aug 13 01:58:36 2003 Z

C:\Windows\system32\dfmgrui.exe

ModTime: Sun Nov 21 03:24:15 2010 Z

Executed

C:\WINDOWS\Installer\MSID252.tmp

ModTime: Wed Apr 20 14:58:45 2016 Z

Executed

C:\WINDOWS\system32\oobe\msoobe.exe

ModTime: Sun Nov 21 03:23:52 2010 Z

## SYSTEM OUTPUT

Executed

C:\Windows\system32\SnippingTool.exe  
ModTime: Tue Jul 14 01:39:41 2009 Z  
Executed

C:\Windows\system32\atiesrxx.exe  
ModTime: Thu Sep 12 02:46:54 2013 Z  
Executed

C:\Windows\System32\colorui.dll  
ModTime: Tue Jul 14 01:40:22 2009 Z

C:\Windows\System32\tsdiscon.exe  
ModTime: Sun Nov 21 03:24:41 2010 Z

C:\Program Files  
(x86)\Google\Update\Install\{261C1A12-8322-468D-AFC2-C80CEBE89959}\50.0.2661.75\_chrome\_installer.exe  
ModTime: Wed Apr 13 01:12:22 2016 Z  
Executed

C:\Windows\SysWOW64\syncui.dll  
ModTime: Sun Nov 21 03:25:09 2010 Z

C:\Program Files\Common Files\McAfee\SystemCore\DAInstall.exe  
ModTime: Mon Apr 18 15:58:25 2016 Z  
Executed

C:\WINDOWS\TEMP\{0ED4EB69-CA7B-4CB4-BF63-E5A8C663D778}\ISBEW64.exe  
ModTime: Mon Apr 18 15:57:37 2016 Z  
Executed

C:\Windows\SysWOW64\twext.dll  
ModTime: Sun Nov 21 03:24:32 2010 Z

C:\Program Files\Common Files\McAfee\Casper\installer.exe  
ModTime: Mon Nov 9 20:22:02 2015 Z  
Executed

C:\WINDOWS\system32\GfxUIEx.exe  
ModTime: Thu Apr 16 19:14:49 2015 Z  
Executed

C:\WINDOWS\system32\mcbuilder.exe  
ModTime: Sun Nov 21 03:24:26 2010 Z  
Executed

## SYSTEM OUTPUT

C:\WINDOWS\system32\igfxCUIService.exe

ModTime: Thu Apr 16 19:14:55 2015 Z

Executed

C:\Program Files (x86)\Nuance\PaperPort\Paprrport.exe

ModTime: Tue Aug 9 22:48:10 2011 Z

Executed

C:\WINDOWS\system32\atbroker.exe

ModTime: Tue Jul 14 01:38:55 2009 Z

Executed

C:\Program Files\Common Files\McAfee\UPDMGR\3.0.6048.2\mcupdutl.exe

ModTime: Wed Nov 4 15:54:54 2015 Z

Executed

C:\WINDOWS\System32\mobsync.exe

ModTime: Sun Nov 21 03:24:51 2010 Z

Executed

C:\Windows\Temp\nsj674F.tmp\FilestoInstall\PEFHelper.exe

ModTime: Mon Dec 14 09:33:24 2015 Z

Executed

C:\PROGRA~1\McAfee\MSC\mcsync.exe

ModTime: Wed Feb 10 11:55:27 2016 Z

Executed

C:\Program Files (x86)\Apple Software Update\SoftwareUpdate.exe

ModTime: Wed Jun 1 21:57:16 2011 Z

Executed

C:\Windows\SysWOW64\DllHost.exe

ModTime: Tue Jul 14 01:14:18 2009 Z

Executed

C:\Users\Nikita\Downloads\widipin.exe

ModTime: Sat Feb 20 02:36:22 2016 Z

Executed

C:\Program Files (x86)\Google\Chrome\Application\50.0.2661.75\Installer\setup.exe

ModTime: Tue Apr 19 20:40:55 2016 Z

Executed

C:\Windows\SysWOW64\sendmail.dll

ModTime: Tue Jul 14 01:16:13 2009 Z

C:\Program Files (x86)\McAfee\SiteAdvisor\Download\s7rs.q.exe

## SYSTEM OUTPUT

ModTime: Wed Mar 30 19:58:17 2016 Z  
Executed

C:\Program Files  
(x86)\Google\Update\Install\{BE30EE67-B767-4F79-8012-E65F13FDE1E2}\chrome\_installer.exe

ModTime: Wed Apr 20 12:59:16 2016 Z  
Executed

C:\Windows\TEMP\005437~1.EXE  
ModTime: Fri Nov 27 14:49:14 2015 Z  
Executed

C:\WINDOWS\system32\verclsid.exe  
ModTime: Tue Jul 14 01:39:49 2009 Z  
Executed

D:\paperport\PP12Installer.exe  
ModTime: Mon Jun 18 06:43:34 2012 Z

C:\Program Files  
(x86)\McAfee\SiteAdvisor\{438506CB-E51F-4937-8CC4-7B18873894C9}\saInst.exe  
ModTime: Tue Apr 12 15:43:08 2016 Z  
Executed

C:\Program Files\WinRAR\WinRAR.exe  
ModTime: Sun Dec 1 18:09:01 2013 Z  
Executed

C:\\_SMSTaskSequence\Packages\FDA00080\5.0.07.0440\Win7CVPN5007\_.CMD  
ModTime: Fri Aug 12 17:38:47 2011 Z

C:\WINDOWS\Installer\MSICBA5.tmp  
ModTime: Mon Apr 18 15:58:25 2016 Z  
Executed

C:\Windows\Temp\nsrB4D1.tmp\FilestoInstall\PEFHelper.exe  
ModTime: Wed Mar 2 17:17:39 2016 Z  
Executed

C:\Program Files  
(x86)\Google\Update\Install\{3D787DB3-914A-46D0-BE31-8295899B4530}\48.0.2564.116\_48.0.2564.109\_chrome\_updater.exe  
ModTime: Thu Feb 18 05:42:00 2016 Z  
Executed

C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\mbamdor.exe  
ModTime: Mon Oct 5 13:48:37 2015 Z

## SYSTEM OUTPUT

Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\acrotray.exe

ModTime: Thu Sep 24 15:41:25 2015 Z

Executed

D:\paperport\PaperPort\setup.exe

ModTime: Mon Jun 18 06:43:38 2012 Z

C:\Program Files\NVIDIA Corporation\Display\nvxdsync.exe

ModTime: Tue Nov 4 01:04:32 2014 Z

Executed

C:\Users\Nikita\AppData\Local\Google\Chrome\User

Data\SwReporter\6.44.4\software\_reporter\_tool.exe

ModTime: Fri Feb 26 17:02:00 2016 Z

Executed

C:\Program Files (x86)\NCH Software\Switch\switch.exe

ModTime: Sat Oct 3 15:49:37 2015 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\{C442782C-47F4-4FB7-B7BB-54C81A3FA1CC}\InstallFlashPlayer.exe

ModTime: Thu Jan 7 22:17:21 2016 Z

Executed

c:\19f4e73b9d7033c49693\install.exe

ModTime: Sat Dec 12 05:11:00 2015 Z

Executed

c:\b51da2a2e71e216407b922aa8c65\Setup.exe

ModTime: Thu Jul 3 11:16:58 2014 Z

Executed

C:\Program Files (x86)\webex\Productivity Tools\ptoneclk.exe

ModTime: Mon Oct 12 06:06:12 2015 Z

C:\WINDOWS\Installer\MSI4BB7.tmp

ModTime: Tue Apr 19 20:41:21 2016 Z

Executed

C:\WINDOWS\ccmcache\4\kb943280\_hklm\_regfix.cmd

ModTime: Mon Jan 27 21:31:55 2014 Z

C:\Windows\System32\mf.dll

ModTime: Tue Feb 3 03:31:01 2015 Z



## SYSTEM OUTPUT

C:\Program Files\Common Files\Microsoft Shared\OFFICE14\msoshext.dll  
ModTime: Tue Jun 25 08:11:24 2013 Z

C:\Program Files (x86)\Audiograbber\lame.exe  
ModTime: Tue Feb 28 21:05:30 2012 Z

C:\Program Files (x86)\Microsoft Office\Office12\EXCEL.EXE  
ModTime: Thu Nov 12 07:29:03 2015 Z  
Executed

C:\Program Files (x86)\Pointsec\Pointsec for PC\fde\_da\_ew.exe  
ModTime: Tue Oct 8 22:56:23 2013 Z  
Executed

D:\setup.exe  
ModTime: Mon Oct 19 18:27:13 2015 Z

C:\Windows\system32\vcsFPSERVICE.exe  
ModTime: Thu Sep 12 12:41:02 2013 Z  
Executed

C:\\_SMSTaskSequence\Packages\PS1002F3\setup\_util\_x64.exe  
ModTime: Thu Jun 25 01:40:10 2015 Z  
Executed

C:\WINDOWS\Installer\MSI25A2.tmp  
ModTime: Mon Apr 18 15:59:54 2016 Z  
Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat Elements\ContextMenu.dll  
ModTime: Thu Sep 24 15:41:01 2015 Z

C:\ProgramData\McAfee\Common  
Framework\Evaluation\VIRUSCAN8800\Patch\7\0000\setup.exe  
ModTime: Mon Apr 18 15:59:39 2016 Z  
Executed

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.exe  
ModTime: Sat Apr 12 03:39:56 2014 Z  
Executed

c:\PROGRA~1\COMMON~1\mcafee\updmgr\307041~1.1\MCUPDA~1.EXE  
ModTime: Mon Dec 14 16:43:44 2015 Z  
Executed

C:\Program Files (x86)\Mozilla Firefox\crashreporter.exe  
ModTime: Thu Jan 7 15:35:47 2016 Z  
Executed

## SYSTEM OUTPUT

C:\Windows\system32\magnify.exe

ModTime: Tue Jul 14 01:39:16 2009 Z

C:\WINDOWS\TEMP\{C012EC36-0D1B-471A-BEF2-C2D5553393BF}\InstallFlashPlayer.exe

ModTime: Wed Apr 20 14:55:58 2016 Z

Executed

C:\\_SMSTaskSequence\Packages\FDA002C1\kb943280\_hklm\_regfix.cmd

ModTime: Mon Jan 27 21:31:55 2014 Z

C:\Windows\SysWOW64\regsvr32.exe

ModTime: Tue Jul 14 01:39:29 2009 Z

Executed

C:\WINDOWS\SysWOW64\Prot\_srv.exe

ModTime: Tue Oct 8 22:56:23 2013 Z

Executed

C:\\_SMSTaskSequence\Packages\FDA000DB\jinit13118\Jinit13118.EXE

ModTime: Tue Feb 1 22:05:38 2005 Z

Executed

C:\Windows\TEMP\009839~1.EXE

ModTime: Fri Nov 27 14:49:14 2015 Z

Executed

C:\WINDOWS\system32\wlrmrdr.exe

ModTime: Tue Jul 14 01:39:55 2009 Z

Executed

c:\3cb5f26f2fc5f9d5c4e783d5be\Setup.exe

ModTime: Sun Jun 12 04:36:34 2011 Z

Executed

C:\Windows\System32\sdclt.exe

ModTime: Sun Nov 21 03:25:06 2010 Z

Executed

C:\Windows\system32\aitagent.EXE

ModTime: Sun Nov 21 03:24:08 2010 Z

Executed

C:\Users\Abe-Arjun

Malik\AppData\Local\Adobe\4C8BAB87-784D-4819-8C69-19F593639E7B\gccheck\_small.exe

ModTime: Sat Feb 6 20:05:36 2016 Z

Executed

## SYSTEM OUTPUT

C:\Windows\twain\_32\BrSc12b\MF9340CDWU\BrTwdFe.ds  
ModTime: Tue May 1 10:20:40 2012 Z

C:\Program Files (x86)\Brother\Firmware\FirmwareUpdater.exe  
ModTime: Tue Oct 9 15:28:06 2012 Z  
Executed

C:\Windows\winhlp32.exe  
ModTime: Sat Nov 29 16:14:45 2014 Z  
Executed

C:\WINDOWS\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe  
ModTime: Mon Apr 18 15:45:08 2016 Z  
Executed

C:\WINDOWS\Explorer.EXE  
ModTime: Sun Nov 21 03:24:11 2010 Z  
Executed

C:\PROGRA~2\WebEx\PRODUC~1\PTIM.exe  
ModTime: Mon Oct 12 06:06:10 2015 Z  
Executed

D:\paperport\Prerequisite\vc redistrib\_x86.exe  
ModTime: Mon Jun 18 06:43:55 2012 Z

C:\WINDOWS\SysWOW64\reg.exe  
ModTime: Tue Jul 14 01:14:30 2009 Z  
Executed

C:\Program Files (x86)\Google\Chrome\Application\chrome.exe  
ModTime: Fri Dec 11 03:54:14 2015 Z  
Executed

C:\Windows\Temp\nsfA9F5.tmp\FilestoInstall\PEFHelper.exe  
ModTime: Wed Mar 2 17:17:39 2016 Z  
Executed

C:\Users\Abe-Arjun.Mallik\Documents\Misc\Downloads\iTunes6464Setup.exe  
ModTime: Thu Oct 22 14:52:45 2015 Z

D:\GlobalSubmitReview\GSReview2014\Sleep\_w7.exe  
ModTime: Mon Aug 15 16:48:17 2011 Z

C:\WINDOWS\system32\runonce.exe  
ModTime: Sun Nov 21 03:24:27 2010 Z  
Executed

## SYSTEM OUTPUT

C:\Program Files (x86)\ControlCenter4\BrCcUxSys.exe  
ModTime: Mon Nov 19 21:30:02 2012 Z  
Executed

C:\Windows\System32\TCPSVCS.EXE  
ModTime: Tue Jul 14 01:39:47 2009 Z

C:\WINDOWS\Microsoft.NET\Framework\v3.5\addinutil.exe  
ModTime: Sun Nov 21 03:24:59 2010 Z  
Executed

C:\WINDOWS\system32\tasklist.exe  
ModTime: Tue Jul 14 01:39:47 2009 Z  
Executed

C:\Windows\System32\SearchFolder.dll  
ModTime: Sun Nov 21 03:24:28 2010 Z

C:\Program Files (x86)\Brother\Brmfl12d\BrScUtil.exe  
ModTime: Tue Aug 28 23:57:16 2012 Z

C:\Windows\system32\userinit.exe  
ModTime: Sun Nov 21 03:24:28 2010 Z  
Executed

C:\Users\Nikita\AppData\Local\Microsoft\Windows\Burn\Burn\SmartGesture\_Win7\_64\_VER22  
14\setup.exe  
ModTime: Mon Mar 31 16:44:14 2014 Z

C:\Program Files\Common Files\McAfee\platform\CommonBuild\McCBEntAndInstru.exe  
ModTime: Thu Nov 26 14:12:13 2015 Z  
Executed

C:\Windows\System32\ieframe.dll  
ModTime: Sun Nov 8 21:14:12 2015 Z

C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE  
ModTime: Wed Nov 18 22:37:14 2015 Z  
Executed

C:\Program Files (x86)\Google\Update\GoogleUpdate.exe  
ModTime: Fri Sep 11 14:56:25 2015 Z  
Executed

C:\Windows\syswow64\Windowspowershell\v1.0\powershell.exe  
ModTime: Tue Jul 14 01:14:24 2009 Z

C:\Program Files (x86)\Google\Update\1.3.28.15\GoogleCrashHandler64.exe

## SYSTEM OUTPUT

ModTime: Tue Apr 19 20:40:07 2016 Z  
Executed

C:\Program Files\Common Files\McAfee\MSGSDK\msgrunner.exe  
ModTime: Thu Nov 5 22:36:38 2015 Z  
Executed

C:\Program Files  
(x86)\McAfee\SiteAdvisor\{438506CB-E51F-4937-8CC4-7B18873894C9}\mcinst.exe  
ModTime: Mon May 4 19:41:42 2015 Z  
Executed

C:\WINDOWS\system32\wbem\wmiprvse.exe  
ModTime: Sun Nov 21 03:24:15 2010 Z  
Executed

C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\VACon64.exe  
ModTime: Wed Mar 12 20:52:14 2014 Z  
Executed

C:\Program Files (x86)\Cisco Systems\Cisco Jabber\wbxcOIE.exe  
ModTime: Thu Aug 7 23:05:36 2014 Z  
Executed

C:\Windows\System32\reg.exe  
ModTime: Tue Jul 14 01:39:29 2009 Z

C:\WINDOWS\TEMP\IE130DF.tmp\IE11-SUPPORT\IENRCORE.EXE  
ModTime: Mon Oct 14 23:27:54 2013 Z  
Executed

C:\Program Files (x86)\Consumer Input\Internet Explorer\dca-host.exe  
ModTime: Thu Feb 11 15:51:03 2016 Z  
Executed

C:\WINDOWS\TEMP\vcredist\_x86\_2010.exe  
ModTime: Fri Nov 22 19:59:18 2013 Z  
Executed

C:\Windows\Installer\{3407ACEE-CEEE-46F3-BDBA-FF1830D4C42D}\\_3ED46C0EFB35798DEEA279.exe  
ModTime: Wed Dec 30 12:23:18 2015 Z

C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE  
ModTime: Wed Nov 11 20:52:22 2015 Z  
Executed

C:\Windows\System32\mssvp.dll

## SYSTEM OUTPUT

ModTime: Sat Nov 29 16:05:18 2014 Z

C:\WINDOWS\Installer\MSICFA4.tmp

ModTime: Mon Apr 18 15:58:26 2016 Z

Executed

C:\Program Files\DellTPad\HidMonitorSvc.exe

ModTime: Thu Apr 16 19:14:31 2015 Z

Executed

C:\WINDOWS\TEMP\maEF8C.tmp\x64\mfehidin.exe

ModTime: Wed Apr 20 13:19:10 2016 Z

Executed

C:\Windows\TEMP\023962~1.EXE

ModTime: Fri Nov 27 14:49:14 2015 Z

Executed

C:\Windows\SoftwareDistribution\Download\Install\ndp45-kb3127229-x64.exe

ModTime: Thu Jan 21 02:07:27 2016 Z

Executed

D:\installmanager\MFC-9340CDW\InstallManager.exe

ModTime: Wed Jun 13 00:03:54 2012 Z

C:\Windows\System32\grpconv.exe

ModTime: Tue Jul 14 01:39:11 2009 Z

Executed

C:\Program Files\HP\HP Photosmart 7520 series\bin\hpwebreg.exe

ModTime: Wed Oct 17 08:38:57 2012 Z

Executed

C:\Windows\System32\systray.exe

ModTime: Tue Jul 14 01:39:47 2009 Z

C:\Users\ad\_dcc\_s.nchotu\AppData\Local\Temp\46EF.tmp\jabber-bootstrap.bat

ModTime: Tue Apr 19 20:41:20 2016 Z

C:\WINDOWS\system32\find.exe

ModTime: Tue Jul 14 01:39:10 2009 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\DLG\exe\7dd4d1054550b7498df9817f9aae33e3\videog  
rabber\_Setup\_product-website\_en-US.exe

ModTime: Sat Feb 20 01:48:56 2016 Z

Executed

## SYSTEM OUTPUT

C:\\_SMSTaskSequence\Packages\FDA000DB\jinit13122\data1.hdr  
ModTime: Tue Apr 5 09:39:20 2005 Z

C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE  
ModTime: Sat Oct 31 09:26:15 2015 Z  
Executed

C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\ngen.exe  
ModTime: Thu Mar 18 17:16:28 2010 Z  
Executed

C:\Windows\Installer\MSIAA6C.tmp  
ModTime: Thu Jan 14 16:37:31 2016 Z  
Executed

C:\Windows\Temp\nskC23C.tmp\FilestoInstall\PEFHelper.exe  
ModTime: Mon Dec 14 09:33:24 2015 Z  
Executed

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe  
ModTime: Sat Apr 12 03:39:56 2014 Z  
Executed

C:\Program Files  
(x86)\McAfee\SiteAdvisor\{C0D0029B-8FFE-4540-B398-1CE31FEABB7D}\mcinst.exe  
ModTime: Mon May 4 20:41:41 2015 Z  
Executed

C:\Windows\System32\ucsvc.exe  
ModTime: Tue Jul 14 01:39:48 2009 Z

D:\paperport\PDFViewer\PDFViewer\setup.exe  
ModTime: Mon Jun 18 06:43:39 2012 Z

C:\Program Files (x86)\McAfee\Common Framework\FrameworkService.exe  
ModTime: Tue Feb 10 20:07:59 2015 Z  
Executed

C:\Program Files\Common Files\McAfee\SystemCore\mfefire.exe  
ModTime: Mon Sep 21 18:31:25 2015 Z  
Executed

c:\PROGRA~2\mcAfee\SITEAD~1\saUpd.exe  
ModTime: Wed Dec 2 15:39:17 2015 Z  
Executed

C:\Program Files (x86)\McAfee\Host Intrusion  
Prevention\vscore\HIP8\_15\_4\_0\x64\mfehidin.exe

## SYSTEM OUTPUT

ModTime: Mon Jun 15 17:22:30 2015 Z  
Executed

C:\WINDOWS\system32\wbem\WmiApSrv.exe  
ModTime: Tue Jul 14 01:39:55 2009 Z  
Executed

C:\Windows\System32\tquery.dll  
ModTime: Sat Nov 29 16:05:18 2014 Z

C:\Program Files (x86)\Windows Mail\WinMail.exe  
ModTime: Tue Jul 14 01:14:45 2009 Z  
Executed

C:\WINDOWS\system32\wuauclt.exe  
ModTime: Fri Nov 20 18:54:15 2015 Z  
Executed

C:\\_SMSTaskSequence\Packages\PS1002EF\osd\_flash20inst\_activex.cmd  
ModTime: Wed Dec 16 19:32:40 2015 Z

C:\Program Files\HP\HP Photosmart 7520 series\Bin\HPNetworkCommunicatorCom.exe  
ModTime: Wed Oct 17 08:27:41 2012 Z  
Executed

C:\Windows\system32\xpsrchvw.exe  
ModTime: Tue Jul 14 01:39:59 2009 Z

C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerPlugin\_20\_0\_0\_267.exe  
ModTime: Thu Jan 7 22:17:25 2016 Z  
Executed

C:\Program Files\HP\HP Photosmart 7520 series\bin\HPDeviceUpdateHost.exe  
ModTime: Wed Oct 17 08:32:35 2012 Z  
Executed

C:\Program Files\DisplayLink Core Software\DisplayLinkUserAgent.exe  
ModTime: Thu Oct 22 20:56:30 2015 Z  
Executed

c:\4f7a8a6edc50d2483adc8a511abde9a6\Setup.exe  
ModTime: Thu Jul 3 11:16:58 2014 Z  
Executed

C:\Windows\system32\sethc.exe  
ModTime: Sun Nov 21 03:24:09 2010 Z  
Executed



## SYSTEM OUTPUT

C:\Program Files (x86)\NCH Software\WavePad\mp3e13.exe

ModTime: Sat Feb 20 13:26:07 2016 Z

Executed

D:\TurboTax 2015\TurboTax 2015 Installer.exe

ModTime: Mon Oct 19 18:27:42 2015 Z

C:\Windows\System32\TsUsbRedirectionGroupPolicyControl.exe

ModTime: Wed Oct 2 02:11:13 2013 Z

C:\Users\AD\_DCC~1.NCH\AppData\Local\Temp\CR\_71467.tmp\setup.exe

ModTime: Tue Apr 19 20:40:55 2016 Z

Executed

C:\Program Files (x86)\Mozilla Firefox\firefox.exe

ModTime: Thu Jan 7 15:35:47 2016 Z

Executed

C:\Windows\TEMP\D48DB75E-EA33-4389-B693-3FB8443D4865\dismhost.exe

ModTime: Sat Nov 29 16:13:49 2014 Z

Executed

C:\Users\Nikita\AppData\Local\Google\Chrome\User  
Data\SwReporter\6.44.3\software\_reporter\_tool.exe

ModTime: Tue Feb 16 21:22:02 2016 Z

Executed

C:\Windows\system32\mmc.exe

ModTime: Tue Jul 14 01:39:19 2009 Z

Executed

C:\Program Files (x86)\Brother\Brmfl12d\OmniJoinTrial.exe

ModTime: Thu Jun 14 15:07:50 2012 Z

Executed

C:\Users\ad\_dcc\_s.nchotu\AppData\Local\Temp\E7EE.tmp\CopyBootstrap.bat

ModTime: Tue Apr 19 20:40:56 2016 Z

C:\Users\AD\_DCC~1.NCH\AppData\Local\Temp\DMT\_Files\TargetPCLauncher.exe

ModTime: Thu Jul 31 04:37:44 2014 Z

Executed

C:\Program Files

(x86)\Google\Update\Install\{B4C5964E-9A1E-4125-9D48-E4706042BDAA}\48.0.2564.97\_47.0  
.2526.111\_chrome\_updater\_3stage.exe

ModTime: Wed Jan 27 11:26:00 2016 Z

Executed

## SYSTEM OUTPUT

C:\Windows\Temp\nsk90F2.tmp\FilestoInstall\PEFHelper.exe

ModTime: Mon Dec 14 09:33:24 2015 Z

Executed

C:\WINDOWS\Installer\MSIEF2F.tmp

ModTime: Tue Apr 19 20:40:58 2016 Z

Executed

C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe

ModTime: Sat Apr 12 04:08:07 2014 Z

Executed

C:\Windows\SysWOW64\EhStorShell.dll

ModTime: Tue Jul 14 01:15:14 2009 Z

C:\Program Files (x86)\Audiograbber\Lame-Uninstall.exe

ModTime: Tue Jan 12 01:31:02 2016 Z

C:\WINDOWS\system32\CompatTelRunner.exe

ModTime: Fri Sep 18 19:22:39 2015 Z

Executed

C:\Windows\System32\wsqmcons.exe

ModTime: Sun Nov 21 03:24:49 2010 Z

Executed

C:\Program Files\Common Files\Microsoft Shared\Ink\InputPersonalization.exe

ModTime: Tue Jul 14 01:39:13 2009 Z

Executed

C:\Windows\Installer\{90140000-0011-0000-0000-00000000FF1CE}\accicons.exe

ModTime: Wed Dec 30 12:57:23 2015 Z

C:\Program Files (x86)\Nuance\PaperPort\pptd40nt.exe

ModTime: Tue Aug 2 21:49:24 2011 Z

Executed

C:\Windows\System32\WUDFHost.exe

ModTime: Sat Nov 29 16:07:20 2014 Z

Executed

C:\Windows\ccmcache\4\reg\_64.exe

ModTime: Tue Jul 14 01:39:30 2009 Z

Executed

C:\WINDOWS\TEMP\7976FD2E-D3DC-4D8E-B437-44CC363D4CE7\dismhost.exe

ModTime: Fri May 30 08:07:49 2014 Z

Executed

## SYSTEM OUTPUT

C:\WINDOWS\Installer\MSI7811.tmp  
ModTime: Mon Apr 18 15:56:59 2016 Z  
Executed

C:\PROGRA~2\McAfee\COMMON~1\McScanCheck.exe  
ModTime: Tue Feb 10 20:07:59 2015 Z  
Executed

C:\Windows\SysWOW64\CScript.exe  
ModTime: Sat Nov 29 15:57:38 2014 Z  
Executed

C:\Windows\Installer\{90140000-0011-0000-0000-00000000FF1CE}\wordicon.exe  
ModTime: Wed Dec 30 12:57:23 2015 Z

C:\WINDOWS\Installer\MSI46C5.tmp  
ModTime: Tue Apr 19 20:41:20 2016 Z  
Executed

C:\Program Files (x86)\Brother\BrUtilities\BrLogRx.exe  
ModTime: Fri Feb 27 21:38:09 2009 Z  
Executed

C:\Program Files (x86)\GUME447.tmp\GoogleUpdate.exe  
ModTime: Tue Apr 19 20:47:28 2016 Z  
Executed

C:\Program Files (x86)\Citrix\ICA Client\wfcrun32.exe  
ModTime: Tue Oct 12 22:28:26 2010 Z  
Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\is-RJURJ.tmp\1clickdvdcopyprosetup5.1.0.6.tmp  
ModTime: Sun Mar 27 20:33:01 2016 Z  
Executed

C:\Windows\system32\rundll32.exe  
ModTime: Tue Jul 14 01:14:31 2009 Z  
Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\is-L2NR7.tmp\1clickdvdcopyprosetup5.1.0.6.tmp  
ModTime: Sun Mar 27 20:33:08 2016 Z  
Executed

C:\Program Files (x86)\McAfee\Common Framework\udaterui.exe  
ModTime: Tue Feb 10 20:07:59 2015 Z  
Executed

## SYSTEM OUTPUT

C:\Program Files (x86)\Nuance\PDF Create 8\bin\GDirectShellExt.dll  
 ModTime: Fri Nov 11 15:16:10 2011 Z

C:\Program Files\DisplayLink Core Software\dlua\_630.exe  
 ModTime: Mon Apr 18 15:37:29 2016 Z  
 Executed

C:\Program Files\McAfee\MSC\mcinfo.exe  
 ModTime: Thu Dec 3 20:15:50 2015 Z  
 Executed

C:\Windows\system32\utilman.exe  
 ModTime: Tue Jul 14 01:39:49 2009 Z  
 Executed

C:\WINDOWS\system32\powershell\powershell.exe  
 ModTime: Tue Jul 14 01:39:20 2009 Z

C:\Users\Abe-Arjun Malik\AppData\Local\Temp\\_is394F.exe  
 ModTime: Wed May 24 17:10:41 2006 Z

C:\Program Files (x86)\Common Files\Apple\Apple Application Support\distnoted.exe  
 ModTime: Fri May 15 20:26:58 2015 Z  
 Executed

C:\Users\AD\_DCC~1.NCH\AppData\Local\Temp\1\GUM209B.tmp\GoogleUpdateSetup.exe  
 ModTime: Fri Oct 2 20:17:22 2015 Z  
 Executed

C:\Windows\Installer\{90140000-0011-0000-0000-00000000FF1CE}\outicon.exe  
 ModTime: Wed Dec 30 12:57:23 2015 Z

C:\Program Files (x86)\McAfee\Common Framework\McTray.exe  
 ModTime: Tue Feb 10 20:07:59 2015 Z  
 Executed

C:\Windows\System32\DeviceCenter.dll  
 ModTime: Sun Nov 21 03:23:51 2010 Z

C:\d3b6e75a1a6e98569619b232\Setup.exe  
 ModTime: Tue Dec 22 03:29:18 2015 Z  
 Executed

C:\WINDOWS\system32\StikyNot.exe  
 ModTime: Tue Jul 14 01:39:46 2009 Z

C:\WINDOWS\CCM\SCNotification.exe  
 ModTime: Tue Apr 14 08:00:00 2015 Z

## SYSTEM OUTPUT

Executed

C:\WINDOWS\system32\\_SMSOSDSetup\TsProgressUI.exe

ModTime: Sun Oct 4 22:04:59 2015 Z

Executed

C:\Windows\bfsvc.exe

ModTime: Sun Nov 21 03:24:22 2010 Z

Executed

C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerPlugin\_19\_0\_0\_226.exe

ModTime: Thu Oct 22 16:42:56 2015 Z

Executed

C:\WINDOWS\system32\msiexec.exe

ModTime: Mon Jun 15 21:42:49 2015 Z

Executed

C:\Windows\SysWOW64\mydocs.dll

ModTime: Sun Nov 21 03:24:15 2010 Z

C:\WINDOWS\system32\taskmgr.exe

ModTime: Sun Nov 21 03:24:24 2010 Z

Executed

C:\Windows\System32\typeperf.exe

ModTime: Mon May 25 18:18:45 2015 Z

C:\Windows\sysWow64\SearchProtocolHost.exe

ModTime: Sat Nov 29 16:05:18 2014 Z

Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\Xtras\AdobePDF\PrintINF64.exe

ModTime: Mon Oct 25 19:13:42 2010 Z

Executed

C:\Windows\Temp\nsk8970.tmp\FilestoInstall\PEFHelper.exe

ModTime: Mon Dec 14 09:33:24 2015 Z

Executed

D:\Launch\_PCRestore.exe

ModTime: Mon Nov 17 16:39:10 2014 Z

C:\Program Files\Common Files\microsoft shared\ink\TabTip.exe

ModTime: Tue Sep 1 18:13:59 2015 Z

Executed

C:\Program Files\Common Files\McAfee\VSore\_15\_4\_1\mfehidin.exe

## SYSTEM OUTPUT

ModTime: Wed Nov 18 19:22:58 2015 Z  
Executed

C:\Windows\System32\EhStorShell.dll  
ModTime: Tue Jul 14 01:40:36 2009 Z

C:\Users\Abe-Arjun  
Malik\AppData\Local\Adobe\979B5697-E226-44C9-8D79-6E5D76AFED00\116A641C-A679-4E5E-AF  
B3-0CC6E5EB4EF8\BC326B9C-08DD-46B9-B762-E73ED332F03A  
ModTime: Thu Jan 7 22:17:19 2016 Z  
Executed

C:\Program Files (x86)\Adobe\Photoshop Elements 2\PhotoshopElements.exe  
ModTime: Thu Sep 10 16:26:23 2015 Z  
Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\{5D609291-3685-4AAC-8681-90B08AE8DB8A}\ISBEW64.  
exe  
ModTime: Thu May 18 23:21:40 2006 Z  
Executed

C:\Windows\SysWOW64\FlashPlayerCPLApp.cpl  
ModTime: Thu Jan 7 22:17:25 2016 Z

C:\Program Files (x86)\Google\Chrome\Application\47.0.2526.111\Installer\setup.exe  
ModTime: Fri Jan 15 16:59:05 2016 Z  
Executed

C:\Windows\SysWOW64\prnflldr.dll  
ModTime: Sun Nov 21 03:24:01 2010 Z

C:\Windows\SysWOW64\audiodev.dll  
ModTime: Sun Nov 21 03:25:10 2010 Z

C:\WINDOWS\system32\OSDSETUPHOOK.EXE  
ModTime: Sun Oct 4 22:04:59 2015 Z  
Executed

C:\Users\Abe-Arjun Malik\Downloads\flashplayer20\_ha\_install.exe  
ModTime: Thu Jan 7 22:02:39 2016 Z  
Executed

C:\\_SMSTaskSequence\Packages\FDA00184\DigiSign.cmd  
ModTime: Tue Sep 4 16:59:26 2012 Z

C:\Program Files (x86)\Citrix\ICA Client\concentr.exe  
ModTime: Tue Oct 12 22:24:38 2010 Z  
Executed

## SYSTEM OUTPUT

C:\Windows\System32\wscui.cpl

ModTime: Tue Jul 14 01:38:52 2009 Z

C:\Windows\system32\SearchProtocolHost.exe

ModTime: Sat Nov 29 16:05:18 2014 Z

Executed

C:\Windows\system32\PrintIsolationHost.exe

ModTime: Tue Jul 14 01:39:27 2009 Z

Executed

C:\WINDOWS\system32\svchost.exe

ModTime: Tue Jul 14 01:39:46 2009 Z

Executed

C:\WINDOWS\system32\Wat\WatAdminSvc.exe

ModTime: Tue Dec 29 20:46:10 2015 Z

Executed

C:\WINDOWS\Installer\MSIA80.tmp

ModTime: Mon Apr 18 15:58:41 2016 Z

Executed

C:\\_SMSTaskSequence\Packages\FDA000C7\Adobe Acrobat X\Setup.exe

ModTime: Tue Nov 2 13:32:10 2010 Z

Executed

C:\Program Files (x86)\QuickTime\QTTask.exe

ModTime: Thu Aug 6 16:42:59 2015 Z

Executed

C:\Program Files (x86)\Vimtag\vimtag.exe

ModTime: Thu Dec 24 02:39:06 2015 Z

Executed

C:\Windows\SoftwareDistribution\Download\Install\EnableTask.exe

ModTime: Fri Nov 20 18:45:40 2015 Z

Executed

C:\WINDOWS\system32\wevtutil.exe

ModTime: Tue Jul 14 01:14:44 2009 Z

Executed

C:\Program Files (x86)\Browny02\BrYNSvc.exe

ModTime: Fri Jul 13 17:07:22 2012 Z

Executed

## SYSTEM OUTPUT

C:\Program Files (x86)\Google\Chrome\Application\48.0.2564.103\Installer\setup.exe  
ModTime: Fri Feb 5 00:21:11 2016 Z  
Executed

D:\Launch\_PCBackup.exe  
ModTime: Mon Nov 17 16:38:16 2014 Z

C:\WINDOWS\system32\schtasks.exe  
ModTime: Sun Nov 21 03:24:26 2010 Z  
Executed

C:\Program Files (x86)\McAfee\SiteAdvisor\McChHost.exe  
ModTime: Wed Dec 2 15:37:57 2015 Z  
Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\is-RV0L0.tmp\RestorePointPRO.exe  
ModTime: Thu Dec 31 21:50:53 2015 Z  
Executed

C:\WINDOWS\SysWOW64\RegisterIEPKEYs.exe  
ModTime: Tue Dec 29 19:21:35 2015 Z  
Executed

C:\Program Files (x86)\Consumer  
Input\Update\Install\{14A67186-37B3-4C3E-921A-AED0D20B97BE}\ciff-3.2.0-12257.exe  
ModTime: Wed Feb 17 21:08:35 2016 Z  
Executed

C:\Program Files (x86)\Nuance\PaperPort\PDFProFiltSrvPP.exe  
ModTime: Tue Aug 2 21:47:26 2011 Z  
Executed

C:\Windows\Installer\MSIFCFC.tmp  
ModTime: Tue Feb 2 00:20:03 2016 Z  
Executed

C:\WINDOWS\system32\enstart64.exe  
ModTime: Mon Apr 18 15:54:18 2016 Z  
Executed

C:\ProgramData\webex\WebEx\1526\WbxDLInst.exe  
ModTime: Fri Sep 11 08:20:04 2015 Z  
Executed

C:\Windows\system32\msiexec.exe  
ModTime: Mon Jun 15 21:44:47 2015 Z  
Executed



## SYSTEM OUTPUT

C:\WINDOWS\Installer\MSICB82.tmp

ModTime: Mon Apr 18 15:58:25 2016 Z

Executed

C:\Program Files (x86)\ControlCenter4\BrTwnAccs.exe

ModTime: Mon Nov 19 21:20:36 2012 Z

Executed

C:\Windows\SysWOW64\ieframe.dll

ModTime: Wed Nov 11 16:00:16 2015 Z

C:\WINDOWS\system32\mstsc.exe

ModTime: Tue Oct 1 23:31:09 2013 Z

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe

ModTime: Sat Nov 29 16:52:42 2014 Z

Executed

C:\b52640f7198288348d5448b81ad5\Setup.exe

ModTime: Thu Dec 10 02:05:28 2015 Z

Executed

C:\Program Files (x86)\Videograbber\FreeYouTubeDownloadManager.exe

ModTime: Wed Jun 4 17:57:24 2014 Z

Executed

C:\WINDOWS\CCM\OSDNetSettings.exe

ModTime: Tue Apr 14 08:00:00 2015 Z

Executed

C:\Windows\system32\igfxsrv.exe

ModTime: Wed Apr 9 20:59:40 2014 Z

Executed

C:\Windows\System32\DfsShlEx.dll

ModTime: Tue Jul 14 01:40:28 2009 Z

C:\Windows\SoftwareDistribution\Download\Install\GWXWU.exe

ModTime: Sat Feb 20 00:11:54 2016 Z

Executed

C:\\_SMSTaskSequence\Packages\FDA00171\dotNetFx40\_Full\_setup.exe

ModTime: Thu Jun 7 18:52:52 2012 Z

Executed

C:\Windows\system32\LogonUI.exe

ModTime: Sun Nov 21 03:24:09 2010 Z

Executed

## SYSTEM OUTPUT

C:\PROGRA~2\MICROS~2\Office12\WINWORD.EXE

ModTime: Thu Dec 10 19:50:06 2015 Z

Executed

C:\WINDOWS\Installer\MSIF9B1.tmp

ModTime: Wed Apr 20 14:58:56 2016 Z

Executed

C:\Program Files

(x86)\Google\Update\Install\{CDBF3CD1-29DD-45BC-B4E6-6F2CB1A973FF}\GoogleUpdateSetup.exe

ModTime: Thu Feb 4 14:13:21 2016 Z

Executed

C:\Windows\SysWOW64\InstallShield\setup.exe

ModTime: Wed Jun 10 21:48:32 2009 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\is-3PH9B.tmp\RestorePoint1CLICK.exe

ModTime: Thu Dec 31 21:50:53 2015 Z

Executed

C:\Program Files (x86)\EMC SourceOne\Offline Access\ExOAAgent.exe

ModTime: Sun Sep 18 18:29:01 2011 Z

Executed

C:\Users\Abe-Arjun Malik\Downloads\Firefox Setup Stub 43.0.3.exe

ModTime: Fri Jan 1 20:51:20 2016 Z

Executed

C:\Program Files\McAfee\VirusScan\MVsInst.exe

ModTime: Fri Jan 8 20:11:10 2016 Z

Executed

C:\Program Files (x86)\McAfee\SiteAdvisor\Download\s4ts.p.exe

ModTime: Thu Apr 14 01:19:24 2016 Z

Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\AcroDist.exe

ModTime: Thu Sep 24 15:41:29 2015 Z

Executed

C:\\_SMSTaskSequence\Packages\FDA0020E\jre-6u38-windows-i586.exe

ModTime: Wed Mar 27 15:14:35 2013 Z

Executed

C:\PROGRA~3\WebEx\WebEx\T30\_TC\CiscoWebexWebService.exe

## SYSTEM OUTPUT

ModTime: Sun Jan 31 16:49:23 2016 Z  
Executed

C:\Windows\system32\GWX\GWX.exe  
ModTime: Tue Dec 8 19:06:56 2015 Z  
Executed

C:\Program Files (x86)\McAfee\Common Framework\masvc.exe  
ModTime: Wed Sep 23 23:57:06 2015 Z  
Executed

C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe  
ModTime: Tue Jul 14 01:14:24 2009 Z  
Executed

C:\Program Files (x86)\McAfee\SiteAdvisor\Download\s1ko.p.exe  
ModTime: Wed Apr 13 19:23:50 2016 Z  
Executed

C:\Windows\Installer\MSI62B2.tmp  
ModTime: Thu Jan 14 16:37:13 2016 Z  
Executed

C:\Windows\system32\wuauc1t.exe  
ModTime: Fri Nov 20 18:54:15 2015 Z  
Executed

C:\Windows\Temp\nsc9484.tmp\FilestoInstall\PEFHelper.exe  
ModTime: Mon Dec 14 09:33:24 2015 Z  
Executed

C:\Program Files\WinZip\WzPreviewer64.exe  
ModTime: Mon Apr 29 21:50:00 2013 Z  
Executed

C:\Users\Nikita\Downloads\.,northsouth,3563805613,-1031684194,TC,0-0,SDJTSwAAAAKEIYI1  
XIcej435gFMQsDqBrEKL3vahWSXXdXH8K-Fn6A2\_webex (1).exe  
ModTime: Sun Jan 31 16:06:07 2016 Z

C:\Program Files (x86)\Renesas Electronics\USB 3.0 Host Controller  
Driver\Application\nusb3utl.exe  
ModTime: Wed Aug 3 17:58:22 2011 Z

C:\Program Files (x86)\Java\jre6\zipper.exe  
ModTime: Sun Oct 11 09:02:28 2009 Z  
Executed

C:\Program Files (x86)\Encore\Hoyle Puzzle and Board Games 2011\Hoyle Puzzle

## SYSTEM OUTPUT

Games.exe

ModTime: Mon Jul 13 21:21:43 2009 Z

Executed

C:\Windows\System32\ExplorerFrame.dll

ModTime: Thu Aug 6 18:06:20 2015 Z

C:\Program Files (x86)\Renesas Electronics\USB 3.0 Host Controller  
Driver\Application\nusb3mon.exe

ModTime: Fri Sep 16 22:39:23 2011 Z

Executed

C:\Program Files (x86)\Nuance\PDF Create 8\RegistryController.exe

ModTime: Wed Jun 13 12:09:50 2012 Z

Executed

C:\WINDOWS\system32\LogonUI.exe

ModTime: Sun Nov 21 03:24:09 2010 Z

Executed

C:\Program Files (x86)\eRoom 7\ERClient7.exe

ModTime: Tue Aug 23 07:44:32 2011 Z

Executed

C:\Windows\servicing\GC64\tzupd.exe

ModTime: Fri Mar 11 17:41:11 2016 Z

Executed

C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\mscorlib.exe

ModTime: Thu Mar 18 17:16:28 2010 Z

Executed

C:\Program Files (x86)\Microsoft Office\Office12\msotmed.exe

ModTime: Thu Feb 26 21:07:12 2009 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\is-OQLLG.tmp\KantoPlayer.tmp

ModTime: Fri Jan 8 19:10:06 2016 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\nsr75A4.tmp

ModTime: Fri Apr 10 12:57:22 2015 Z

Executed

C:\WINDOWS\System32\msdtc.exe

ModTime: Tue Jul 14 01:39:21 2009 Z

Executed

## SYSTEM OUTPUT

C:\Windows\SysWOW64\wmpshell.dll  
ModTime: Sun Nov 21 03:25:10 2010 Z

C:\Windows\system32\wevtutil.exe  
ModTime: Tue Jul 14 01:39:51 2009 Z  
Executed

C:\WINDOWS\system32\displayswitch.exe  
ModTime: Tue Jul 14 01:39:06 2009 Z

C:\Windows\System32\zipfldr.dll  
ModTime: Sun Nov 21 03:24:01 2010 Z

C:\Windows\system32\services.exe  
ModTime: Mon Apr 13 03:28:33 2015 Z  
Executed

C:\WINDOWS\ccmcache\1\ccmsetup.exe  
ModTime: Sun Oct 4 22:04:59 2015 Z  
Executed

C:\Windows\System32\dpapimig.exe  
ModTime: Tue Jul 14 01:39:07 2009 Z  
Executed

C:\Windows\system32\consent.exe  
ModTime: Thu Jun 25 09:58:20 2015 Z  
Executed

C:\Program Files\DisplayLink Core Software\DisplayLinkManager.exe  
ModTime: Thu Oct 22 20:56:28 2015 Z  
Executed

C:\Windows\System32\control.exe  
ModTime: Tue Jul 14 01:39:01 2009 Z  
Executed

C:\Program Files  
(x86)\McAfee\SiteAdvisor\{2251B01E-9847-4E97-A8BF-FE932C84BCF9}\saInst.exe  
ModTime: Mon Mar 28 17:31:33 2016 Z  
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB3097994-x64.exe  
ModTime: Thu Mar 10 20:16:37 2016 Z  
Executed

C:\Program Files (x86)\Common Files\Check Point\UIFramework\cptray.exe  
ModTime: Wed Jun 2 18:04:59 2010 Z

## SYSTEM OUTPUT

Executed

C:\WINDOWS\TEMP\{5CA23B93-6D15-48E6-9C39-18FFA4CD5B0C}\ISBEW64.exe

ModTime: Mon Apr 18 16:00:10 2016 Z

Executed

C:\Program Files (x86)\McAfee\Temp\qxz8451\mccertupd.exe

ModTime: Mon Dec 7 05:06:04 2015 Z

Executed

C:\Windows\System32\devmgr.dll

ModTime: Tue Jul 14 01:40:28 2009 Z

C:\Program Files (x86)\QuickTime\QuickTimePlayer.exe

ModTime: Mon Aug 10 16:17:26 2015 Z

C:\caa7e401023c173f9ecc7f\Setup.exe

ModTime: Fri Feb 5 07:13:44 2016 Z

Executed

C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\aspnet\_regiis.exe

ModTime: Thu Mar 18 20:47:22 2010 Z

Executed

C:\Program Files\McAfee\MSC\McInstru.exe

ModTime: Fri Sep 25 16:20:50 2015 Z

Executed

C:\Windows\SysWOW64\FlashPlayerInstaller.exe

ModTime: Tue Jan 19 21:17:52 2016 Z

Executed

C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat Elements\ContextMenu64.dll

ModTime: Thu Sep 24 15:40:41 2015 Z

C:\Program Files (x86)\Windows Media Player\WMPNSSUI.dll

ModTime: Tue Jul 14 01:16:19 2009 Z

C:\WINDOWS\SoftwareDistribution\Download\Install\NDP40-KB3074547-x64.exe

ModTime: Thu Mar 10 20:37:28 2016 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\{BF61A71C-889D-4167-86ED-1517EA86EF82}\ISBEW64.exe

ModTime: Tue Feb 2 00:22:34 2016 Z

Executed

C:\Windows\System32\TpmInit.exe

## SYSTEM OUTPUT

ModTime: Tue Jul 14 01:39:47 2009 Z

C:\WINDOWS\TEMP\\_ISTMP1.DIR\\_INS5176.\_MP

ModTime: Mon Apr 18 15:53:28 2016 Z

Executed

C:\Users\Abe-Arjun Malik\Downloads\BrMain482.exe

ModTime: Tue Feb 2 00:52:20 2016 Z

Executed

C:\Windows\System32\sdiagnhost.exe

ModTime: Tue Jul 14 01:39:37 2009 Z

Executed

C:\\_SMSTaskSequence\Packages\PS1001D8\ciscoanyconnect\_copy\_fdauseripsecprof.cmd

ModTime: Fri Apr 10 16:59:10 2015 Z

C:\Program Files\Common Files\McAfee\SystemCore\ScriptSn.20160418115830.dll

ModTime: Mon Apr 18 15:58:25 2016 Z

C:\WINDOWS\TEMP\InstallAX\_21\_0\_0\_182.exe

ModTime: Mon Mar 7 21:00:26 2016 Z

Executed

C:\Windows\System32\mydocs.dll

ModTime: Sun Nov 21 03:24:01 2010 Z

C:\Program Files (x86)\McAfee\VirusScan Enterprise\VSCore\DAInstall.exe

ModTime: Mon Apr 18 15:58:24 2016 Z

Executed

C:\Program Files (x86)\Consumer Input\Monitoring\cookie-retriever.exe

ModTime: Tue Feb 9 09:28:32 2016 Z

C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\vpnui.exe

ModTime: Wed Mar 12 20:52:32 2014 Z

Executed

C:\Users\AD\_DCC~1.NCH\AppData\Local\Temp\DMT\_Files\MoveMouse.exe

ModTime: Fri Feb 17 02:36:22 2012 Z

Executed

C:\Windows\Installer\{FFD1F7F1-1AC9-4BC4-A908-0686D635ABAF}\AppleSoftwareUpdateIco.exe

ModTime: Thu Jan 7 22:10:27 2016 Z

C:\Program Files\Common

Files\McAfee\AMContent\scanners\x86\_64\datrep\21.0\mcdatarep.exe

## SYSTEM OUTPUT

ModTime: Thu Dec 10 02:48:14 2015 Z  
Executed

C:\WINDOWS\Installer\MSI2572.tmp  
ModTime: Mon Apr 18 15:59:54 2016 Z  
Executed

C:\WINDOWS\servicing\TrustedInstaller.exe  
ModTime: Sun Nov 21 03:24:03 2010 Z  
Executed

C:\\_SMSTaskSequence\Packages\PS10018C\Uninstx64.exe  
ModTime: Thu Jan 16 00:08:00 2014 Z  
Executed

C:\Windows\System32\xcopy.exe  
ModTime: Tue Jul 14 01:39:58 2009 Z  
Executed

C:\WINDOWS\TEMP\vcredist\_x86\_2005.exe  
ModTime: Thu Jun 14 15:05:20 2012 Z  
Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\is-R9QMM.tmp\1clickdvdcopysetup6.1.0.6.tmp  
ModTime: Fri Apr 8 11:34:39 2016 Z  
Executed

C:\Windows\SysWOW64\explorer.exe  
ModTime: Sat Nov 29 16:04:56 2014 Z  
Executed

C:\Windows\System32\sendmail.dll  
ModTime: Tue Jul 14 01:41:53 2009 Z

C:\Windows\SysWOW64\at.exe  
ModTime: Tue Jul 14 01:14:12 2009 Z  
Executed

C:\Windows\System32\rshx32.dll  
ModTime: Tue Jul 14 01:41:53 2009 Z

C:\WINDOWS\Installer\MSIA60.tmp  
ModTime: Mon Apr 18 15:58:41 2016 Z  
Executed

C:\Windows\UDI\AppInstall.exe  
ModTime: Thu Aug 30 17:06:36 2012 Z  
Executed



## SYSTEM OUTPUT

C:\WINDOWS\system32\getmac.exe  
ModTime: Tue Jul 14 01:39:11 2009 Z  
Executed

C:\Windows\System32\powercfg.exe  
ModTime: Tue Jul 14 01:39:27 2009 Z  
Executed

C:\PROGRA~2\McAfee\MSC\MCHlp32.exe  
ModTime: Thu Dec 3 20:15:22 2015 Z  
Executed

C:\WINDOWS\system32\atashost.exe  
ModTime: Fri Sep 11 08:19:50 2015 Z

C:\WINDOWS\WinSxS\x86\_microsoft-windows-ie-gc-registeriepkeys\_31bf3856ad364e35\_11.2.9600.16428\_none\_ae214da780801b0f\RegisterIEPKEYs.exe  
ModTime: Tue Dec 29 19:21:35 2015 Z  
Executed

C:\WINDOWS\Installer\MSI66D0.tmp  
ModTime: Mon Apr 18 15:56:54 2016 Z  
Executed

C:\Windows\TEMP\007014~1.EXE  
ModTime: Mon May 4 20:41:41 2015 Z  
Executed

D:\GoToMeeting Codec\g2m\_codec.exe  
ModTime: Thu Sep 12 18:35:04 2013 Z

C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice\_tmp.exe  
ModTime: Thu Mar 31 23:06:02 2016 Z  
Executed

C:\Program Files (x86)\Cisco Systems\Cisco IP Communicator\communicatork9.exe  
ModTime: Tue Feb 12 18:14:38 2013 Z  
Executed

C:\Windows\system32\mfefvtps.exe  
ModTime: Mon Sep 21 18:33:33 2015 Z  
Executed

C:\Program Files\ActivIdentity\ActivClient\acsagent.exe  
ModTime: Wed Jun 3 21:35:56 2009 Z  
Executed

## SYSTEM OUTPUT

C:\Windows\Microsoft.NET\Framework\v3.5\addinutil.exe

ModTime: Sun Nov 21 03:24:59 2010 Z

Executed

C:\Windows\syswow64\MsiExec.exe

ModTime: Mon Jun 15 21:42:49 2015 Z

Executed

C:\WINDOWS\SYSTEM32\WISPTIS.EXE

ModTime: Sun Nov 21 03:25:10 2010 Z

Executed

C:\Windows\TEMP\CR\_D4D16.tmp\setup.exe

ModTime: Fri Feb 19 22:18:57 2016 Z

Executed

C:\Program Files

(x86)\Google\Update\Install\{C2D88CF0-7ACE-487A-AFB9-09001DC35F2C}\GoogleUpdateSetup.exe

ModTime: Wed Jan 20 17:58:00 2016 Z

Executed

C:\WINDOWS\TEMP\Microsoft .NET Framework 4 Setup\_4.0.30319\TMP2FFE.tmp.exe

ModTime: Thu Mar 18 23:32:37 2010 Z

Executed

C:\Windows\System32\sbe.dll

ModTime: Sat Nov 29 15:52:02 2014 Z

C:\WINDOWS\ccmsetup\ccmsetup.exe

ModTime: Sun Oct 4 22:04:59 2015 Z

Executed

c:\PROGRA~1\COMMON~1\mcafee\updmgr\308053~1.4\MCUPDA~1.EXE

ModTime: Thu Mar 3 15:27:20 2016 Z

Executed

C:\PROGRA~2\COMMON~1\INSTAL~1\Engine\6\INTEL3~1\IKernel.exe

ModTime: Wed Sep 5 07:24:00 2001 Z

Executed

C:\Program Files\McAfee\Gkp\firesvc.exe

ModTime: Tue Jan 5 23:34:48 2016 Z

Executed

C:\Program Files (x86)\Cisco Systems\VPN Client\VAInst64.exe

ModTime: Fri Mar 4 16:51:21 2011 Z

Executed

## SYSTEM OUTPUT

C:\Program Files\mcafee.com\agent\McUpdate.exe

ModTime: Thu Dec 3 20:15:56 2015 Z

Executed

C:\Program Files (x86)\QuickTime\QTSystem\QuickTime.cpl

ModTime: Mon Aug 10 16:16:48 2015 Z

C:\PROGRA~1\McAfee\MSC\McSync.exe

ModTime: Thu Dec 3 20:15:56 2015 Z

Executed

C:\WINDOWS\CCM\CcmExec.exe

ModTime: Tue Apr 14 08:00:00 2015 Z

Executed

C:\Users\Abe-Arjun Malik\Downloads\download-videograbber.exe

ModTime: Sat Feb 20 01:45:01 2016 Z

Executed

C:\Windows\system32\cmd.exe

ModTime: Sun Nov 21 03:23:55 2010 Z

Executed

C:\Program Files (x86)\Hp\HP Software Update\HPWUcli.exe

ModTime: Wed Jun 5 12:46:55 2013 Z

Executed

C:\Users\AD\_DCC~1.NCH\AppData\Local\Temp\1\GUM209B.tmp\GoogleUpdate.exe

ModTime: Tue Apr 19 20:40:05 2016 Z

Executed

C:\WINDOWS\system32\compattel\DiagTrackRunner.exe

ModTime: Wed Jun 3 20:17:05 2015 Z

Executed

C:\Windows\Temp\nso4B56.tmp\FilestoInstall\PEFHelper.exe

ModTime: Wed Mar 2 17:17:39 2016 Z

Executed

C:\Program Files (x86)\Common Files\ScanSoft Shared\PDF8\PDFAttachHelper.exe

ModTime: Wed Jun 13 12:10:26 2012 Z

Executed

C:\Windows\System32\TSTheme.exe

ModTime: Tue Jul 14 01:39:48 2009 Z

C:\Program Files\Common Files\Microsoft

## SYSTEM OUTPUT

Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE

ModTime: Sun Jan 10 01:34:24 2010 Z

Executed

C:\Program Files (x86)\Microsoft Silverlight\5.1.41212.0\coregen.exe

ModTime: Sat Dec 12 04:12:28 2015 Z

Executed

C:\Program Files

(x86)\Google\Update\Install\{0A4C9ADE-33F1-4DE0-93C2-6284D14762F6}\48.0.2564.103\_48.0.2564.97\_chrome\_updater\_3stage.exe

ModTime: Wed Feb 3 00:46:59 2016 Z

Executed

c:\PROGRA~1\mcafee\mpf\mpfalert.exe

ModTime: Tue Jan 5 23:31:22 2016 Z

Executed

C:\Windows\SoftwareDistribution\Download\Install\Windows-KB890830-x64-V5.34-delta.exe

ModTime: Thu Mar 3 00:11:33 2016 Z

Executed

C:\Program Files\Common Files\McAfee\HackerWatch\HWUpdChk.exe

ModTime: Tue Oct 27 21:03:22 2015 Z

Executed

C:\Program Files\Common Files\McAfee\ClientAnalytics\ClientAnalyticsReg.exe

ModTime: Fri Jan 8 15:48:42 2016 Z

Executed

C:\Program Files (x86)\McAfee\SiteAdvisor\Download\s3n4.u.exe

ModTime: Wed Mar 23 21:30:26 2016 Z

Executed

C:\WINDOWS\system32\SearchProtocolHost.exe

ModTime: Wed May 4 05:19:28 2011 Z

Executed

C:\Windows\SoftwareDistribution\Download\Install\Windows-KB890830-x64-V5.35-delta.exe

ModTime: Thu Apr 7 03:00:18 2016 Z

Executed

C:\Program Files\DellTPad\ApMsgFwd.exe

ModTime: Thu Apr 16 19:14:31 2015 Z

Executed

## SYSTEM OUTPUT

C:\WINDOWS\SysWOW64\sc.exe

ModTime: Tue Jul 14 01:14:35 2009 Z

Executed

c:\PROGRA~2\mcafee\SITEAD~1\saoemmgr.exe

ModTime: Tue Dec 29 20:56:26 2015 Z

Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\VSCore\x64\DAInstall.exe

ModTime: Mon Apr 18 15:58:25 2016 Z

Executed

C:\Windows\System32\cscui.dll

ModTime: Sun Nov 21 03:24:41 2010 Z

C:\Windows\SysWOW64\cmd.exe

ModTime: Sun Nov 21 03:24:03 2010 Z

Executed

C:\WINDOWS\TEMP\Microsoft .NET Framework 4 Setup\_4.0.30319\TMPCC93.tmp.exe

ModTime: Fri Mar 19 00:51:07 2010 Z

Executed

c:\922c3e20b4e138d3473990\Setup.exe

ModTime: Thu Feb 5 09:15:53 2015 Z

Executed

C:\Windows\SysWOW64\wpdshext.dll

ModTime: Thu Jan 29 03:02:08 2015 Z

C:\WINDOWS\TEMP\mfeC300.tmp\FrmInst.exe

ModTime: Tue Jun 25 20:08:00 2013 Z

Executed

C:\WINDOWS\system32\net.exe

ModTime: Tue Jul 14 01:39:25 2009 Z

Executed

C:\Program Files (x86)\Google\Google Earth\client\googleearth.exe

ModTime: Thu May 21 05:11:04 2015 Z

Executed

C:\WINDOWS\System32\RegisterIEPKEYs.exe

ModTime: Tue Dec 29 19:21:35 2015 Z

Executed

C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\regasm.exe

ModTime: Thu Mar 20 22:50:32 2014 Z

## SYSTEM OUTPUT

Executed

C:\Program Files (x86)\Mozilla Firefox\updater.exe

ModTime: Fri Feb 12 15:10:26 2016 Z

Executed

C:\Windows\system32\gwx\gwx.exe

ModTime: Wed Feb 17 14:07:29 2016 Z

Executed

C:\Users\Abe-Arjun Malik\Downloads\FitbitConnect\_Win\_20151028\_2.0.1.6742.exe

ModTime: Thu Jan 14 22:00:17 2016 Z

Executed

C:\Windows\TEMP\{F0D555A3-8573-4C4F-89BA-BDBC6F80A35D}\InstallFlashPlayer.exe

ModTime: Tue Jan 19 21:17:54 2016 Z

Executed

C:\\_SMSTaskSequence\Packages\PS1002F3\McAfeeHIP\_ClientSetup.exe

ModTime: Thu Aug 20 17:53:48 2015 Z

Executed

C:\Windows\Microsoft.NET\Framework64\v2.0.50727\cvtres.exe

ModTime: Sat Nov 29 16:52:42 2014 Z

Executed

C:\Windows\Installer\MSI7F96.tmp

ModTime: Thu Jan 14 16:38:26 2016 Z

Executed

C:\WINDOWS\Installer\MSIB1F4.tmp

ModTime: Wed Apr 20 14:58:37 2016 Z

Executed

C:\Windows\System32\Display.dll

ModTime: Sat Nov 29 16:09:44 2014 Z

C:\Users\Nikita\Downloads\SmartGesture\_Win7\_64\_VER2214\setup.exe

ModTime: Mon Mar 31 16:44:14 2014 Z

C:\Windows\system32\compattelrunner.exe

ModTime: Fri Sep 18 19:22:39 2015 Z

Executed

C:\Windows\SysWOW64\WerFault.exe

ModTime: Tue Jul 14 01:14:44 2009 Z

Executed

## SYSTEM OUTPUT

C:\Windows\system32\FlashPlayerInstaller.exe

ModTime: Tue Jan 19 21:17:52 2016 Z

C:\WINDOWS\system32\{A6D608F0-0BDE-491A-97AE-5C4B05D86E01}.bat

ModTime: Tue Apr 19 19:48:37 2016 Z

C:\Program Files (x86)\Java\jre6\bin\jusched.exe

ModTime: Mon Apr 18 15:54:07 2016 Z

Executed

C:\\_SMSTaskSequence\Packages\PS10022F\FramPkg\_4.8.0.1938\_FDSWV04575.exe

ModTime: Thu Jun 11 17:13:49 2015 Z

Executed

C:\Windows\System32\gameux.dll

ModTime: Sat Nov 29 16:09:22 2014 Z

C:\Windows\system32\explorer.exe

ModTime: Sat Nov 29 16:04:56 2014 Z

C:\Users\ABE-AR~1\AppData\Local\Temp\compete.exe

ModTime: Sat Feb 20 01:46:04 2016 Z

Executed

C:\WINDOWS\WinSxS\x86\_microsoft-windows-i...-setieinstalleddate\_31bf3856ad364e35\_11.2.9600.16428\_none\_8eaf79351dba1b94\SetIEInstalledDate.exe

ModTime: Tue Dec 29 19:21:35 2015 Z

Executed

C:\Program Files (x86)\Google\Update\1.3.28.15\GoogleUpdateOnDemand.exe

ModTime: Tue Apr 19 20:40:07 2016 Z

Executed

C:\windows\System32\WUDFHost.exe

ModTime: Thu Jul 26 03:08:53 2012 Z

Executed

C:\WINDOWS\SYSTEM32\IEUNATT.EXE

ModTime: Fri Nov 6 19:05:38 2015 Z

Executed

C:\Users\Abe-Arjun Malik\Downloads\WirelessSetupHelper1.3.3\_enus.exe

ModTime: Tue Feb 2 00:46:43 2016 Z

Executed

C:\Windows\system32\Dwm.exe

ModTime: Tue Jul 14 01:39:08 2009 Z

Executed

## SYSTEM OUTPUT

C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe

ModTime: Sat Nov 29 16:52:45 2014 Z

Executed

C:\Program Files (x86)\McAfee\Host Intrusion Prevention\HipMgmt.exe

ModTime: Thu Jun 25 01:31:22 2015 Z

Executed

C:\Windows\system32\DllHost.exe

ModTime: Tue Jul 14 01:39:06 2009 Z

Executed

C:\Windows\system32\DeviceDisplayObjectProvider.exe

ModTime: Tue Jul 14 01:39:02 2009 Z

Executed

C:\Program Files\McAfee\VirusScan\mcods.exe

ModTime: Tue Oct 20 23:13:26 2015 Z

Executed

D:\installmanager\MFC-9340CDW\BrLogRx.exe

ModTime: Fri Feb 27 07:38:09 2009 Z

C:\Windows\UDI\OSDResults.exe

ModTime: Thu Aug 30 17:06:36 2012 Z

Executed

C:\WINDOWS\SYSTEM32\RUNDLL32.EXE

ModTime: Tue Jul 14 01:39:31 2009 Z

Executed

C:\WINDOWS\System32\Wbem\WMIC.exe

ModTime: Tue Jul 14 01:14:46 2009 Z

C:\Windows\Temp\nsiE860.tmp\FilestoInstall\PEFHelper.exe

ModTime: Mon Dec 14 09:33:24 2015 Z

Executed

c:\Program Files (x86)\Microsoft Silverlight\5.1.41212.0\agcp.exe

ModTime: Sat Dec 12 04:12:28 2015 Z

Executed

C:\Program Files

(x86)\McAfee\SiteAdvisor\{3CDA9858-A1AF-4912-95A3-FFFDE8887928}\mcinst.exe

ModTime: Mon May 4 19:41:42 2015 Z

Executed



## SYSTEM OUTPUT

C:\WINDOWS\Installer\MSIA4F.tmp

ModTime: Mon Apr 18 15:58:41 2016 Z

Executed

C:\ProgramData\FLEXnet\Connect\11\isuspm.exe

ModTime: Tue May 5 21:06:05 2009 Z

Executed

c:\PROGRA~1\mcafee\msc\mcsvrnt.exe

ModTime: Thu Dec 3 20:15:54 2015 Z

Executed

C:\Program Files (x86)\Java\jre6\bin\javaw.exe

ModTime: Mon Apr 18 15:54:07 2016 Z

Executed

C:\Program Files (x86)\Windows Photo Viewer\PhotoViewer.dll

ModTime: Sun Nov 21 03:25:14 2010 Z

C:\Windows\system32\wbengine.exe

ModTime: Sun Nov 21 03:25:14 2010 Z

Executed

C:\Program Files\Common Files\McAfee\SystemCore\mfemms.exe

ModTime: Wed Oct 21 15:29:22 2015 Z

Executed

C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamscheduler.exe

ModTime: Thu Mar 10 18:07:28 2016 Z

Executed

C:\Program Files (x86)\Consumer

Input\Update\Install\{5185F5CC-AF9B-4C07-BC4D-CC577A132A3C}\ciie-3.2.0-12477.exe

ModTime: Wed Feb 17 21:08:35 2016 Z

Executed

C:\Windows\System32\syncui.dll

ModTime: Sun Nov 21 03:24:51 2010 Z

C:\Windows\SysWOW64\plugincpl13126.cpl

ModTime: Tue May 16 08:49:59 2006 Z

C:\WINDOWS\system32\spssvc.exe

ModTime: Sun Nov 21 03:23:56 2010 Z

Executed

C:\Windows\system32\displayswitch.exe

ModTime: Tue Jul 14 01:39:06 2009 Z

## SYSTEM OUTPUT

C:\Users\Abe-Arjun

Malik\AppData\Local\Temp\{5D609291-3685-4AAC-8681-90B08AE8DB8A}\{E98A9C92-E767-475B-8BC6-8780A86DDC72}\BrWIARegRepair.exe

ModTime: Sat Oct 9 00:07:48 2004 Z

Executed

C:\Windows\System32\SystemPropertiesProtection.exe

ModTime: Tue Jul 14 01:39:47 2009 Z

C:\WINDOWS\CCM\TsProgressUI.exe

ModTime: Tue Apr 14 08:00:00 2015 Z

Executed

C:\Program Files (x86)\Cisco Systems\Cisco IP Communicator\CDP\certmgr.exe

ModTime: Fri Mar 18 18:12:34 2011 Z

Executed

C:\Program Files (x86)\Nuance\PDF Create 8\Ereg\Ereg.exe

ModTime: Tue Sep 6 18:47:52 2011 Z

Executed

D:\install\Data\Disk1\Setup.exe

ModTime: Wed May 24 17:10:41 2006 Z

C:\WINDOWS\CCM\tsenv.exe

ModTime: Tue Apr 14 08:00:00 2015 Z

Executed

U C:\Program Files (x86)\HP\HP Photosmart 7520 series\bin\HPScan.exe

ModTime: Wed Oct 17 08:10:52 2012 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\is-GRJB8.tmp\DVD43\_Plugin\_Setup\_1.0.0.6.tmp

ModTime: Sun Mar 27 20:36:11 2016 Z

Executed

C:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\regtlbiv12.exe

ModTime: Thu Mar 18 18:27:13 2010 Z

Executed

C:\\_SMSTaskSequence\WDPackage\fdascripts\ClearOfficeInitials\ClearOfficeInitials.cmd

ModTime: Fri Apr 11 11:24:09 2014 Z

C:\Windows\SysWOW64\acppage.dll

ModTime: Sun Nov 21 03:24:32 2010 Z

C:\WINDOWS\CCM\smsboot.exe

## SYSTEM OUTPUT

ModTime: Tue Apr 14 08:00:00 2015 Z  
Executed

C:\Windows\SysWOW64\zipfldr.dll  
ModTime: Sun Nov 21 03:24:09 2010 Z

C:\Program Files (x86)\Common Files\Apple\Mobile Device  
Support\AppleMobileBackup.exe  
ModTime: Wed Oct 7 16:43:39 2015 Z  
Executed

C:\Windows\ehome\ehshell.exe  
ModTime: Tue Jul 14 01:39:09 2009 Z

C:\Windows\System32\TRACERT.EXE  
ModTime: Tue Jul 14 01:39:48 2009 Z

C:\WINDOWS\system32\wbem\mofcomp.exe  
ModTime: Tue Jul 14 01:39:20 2009 Z  
Executed

C:\Windows\Installer\{789A5B64-9DD9-4BA5-915A-F0FC0A1B7BFE}\AppleSoftwareUpdateIco.e  
xe  
ModTime: Fri Sep 11 17:59:18 2015 Z

C:\Program Files (x86)\Common Files\McAfee\SystemCore\DAInstall.exe  
ModTime: Mon Apr 18 15:58:24 2016 Z  
Executed

C:\WINDOWS\SysWow64\IntelCpHeciSvc.exe  
ModTime: Thu Apr 16 19:14:55 2015 Z  
Executed

C:\Windows\TEMP\022172~1.EXE  
ModTime: Fri Nov 27 14:49:14 2015 Z  
Executed

C:\WINDOWS\SYSTEM32\MUIUNATTEND.EXE  
ModTime: Tue Jul 14 01:39:24 2009 Z  
Executed

C:\WINDOWS\Installer\MSIAB0.tmp  
ModTime: Mon Apr 18 15:58:41 2016 Z  
Executed

C:\Windows\System32\shdocvw.dll  
ModTime: Sat Nov 29 16:12:06 2014 Z

## SYSTEM OUTPUT

C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleUpdateOnDemand.exe  
ModTime: Thu Feb 4 14:13:21 2016 Z  
Executed

C:\Windows\SysWOW64\ntshrui.dll  
ModTime: Sat Nov 29 16:06:06 2014 Z

C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\InstallUtil.exe  
ModTime: Thu Mar 20 22:50:30 2014 Z  
Executed

C:\WINDOWS\system32\SearchFilterHost.exe  
ModTime: Wed May 4 05:19:28 2011 Z  
Executed

C:\WINDOWS\CCM\smsswd.exe  
ModTime: Thu Jun 25 22:15:00 2015 Z  
Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\mcupdate.exe  
ModTime: Thu Jan 16 00:08:00 2014 Z  
Executed

C:\Program Files\Common Files\McAfee\Platform\McAMTaskAgent.exe  
ModTime: Tue Jan 5 15:47:48 2016 Z  
Executed

C:\\_SMSTaskSequence\WDPackage\FDAscripts\ClearOfficeInitials\reg.exe  
ModTime: Mon Apr 14 00:12:32 2008 Z  
Executed

C:\Users\AD\_DCC~1.NCH\AppData\Local\Temp\1\7zS4ECB.tmp\setup.exe  
ModTime: Wed Mar 16 01:50:15 2016 Z  
Executed

C:\Program Files (x86)\Cisco Systems\VPN Client\cvpnd.exe  
ModTime: Fri Mar 4 16:45:07 2011 Z  
Executed

C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility  
Client\InstallHelper.exe  
ModTime: Wed Mar 12 20:52:08 2014 Z  
Executed

C:\Program Files (x86)\SoftwareUpdater\SoftwareUpdater.Bootstrapper.exe  
ModTime: Wed Jun 4 17:57:24 2014 Z  
Executed

## SYSTEM OUTPUT

C:\WINDOWS\system32\rundll32.exe

ModTime: Tue Jul 14 01:14:31 2009 Z

D:\install\data\Disk1\data1.hdr

ModTime: Fri Dec 7 08:34:00 2012 Z

C:\Windows\system32\prevhost.exe

ModTime: Sat Nov 29 16:04:46 2014 Z

Executed

C:\Program Files (x86)\Cisco Systems\Cisco Jabber\x64\wbxcOIE64.exe

ModTime: Thu Jul 24 16:57:25 2014 Z

Executed

C:\Program Files (x86)\McAfee\VirusScan Enterprise\SHSTAT.EXE

ModTime: Thu Jan 16 00:08:00 2014 Z

Executed

C:\Program Files (x86)\McAfee\Common Framework\maconfig.exe

ModTime: Wed Sep 23 23:56:54 2015 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\Setup.exe

ModTime: Wed Oct 28 13:13:02 2015 Z

Executed

C:\Program Files (x86)\Mozilla Firefox\uninstall\helper.exe

ModTime: Thu Jan 7 15:35:45 2016 Z

Executed

C:\Program Files\Common Files\McAfee\UPDMGR\3.0.7041.1\mcupdutl.exe

ModTime: Mon Dec 14 16:43:46 2015 Z

Executed

C:\Program Files\HP\HP Photosmart 7520 series\Bin\SendAFax.exe

ModTime: Wed Oct 17 08:36:11 2012 Z

Executed

C:\PROGRA~1\COMMON~1\DETERM~1\DNE\dnes64x.exe

ModTime: Sun Nov 16 22:39:43 2008 Z

Executed

C:\ProgramData\webex\WebEx\1526\WbxDLDrv.exe

ModTime: Fri Sep 11 08:20:04 2015 Z

Executed

C:\WINDOWS\SYSTEM32\DJJOIN.EXE

ModTime: Sun Nov 21 03:24:09 2010 Z

## SYSTEM OUTPUT

Executed

C:\Program Files (x86)\Consumer  
Input\Update\1.3.25.309\ConsumerInputCrashHandler.exe  
ModTime: Sat Feb 20 01:46:11 2016 Z  
Executed

C:\\_SMSTaskSequence\Packages\PS10009B\OSDActivClientHotfix.cmd  
ModTime: Fri Jan 31 01:19:04 2014 Z

C:\Windows\WinSxS\amd64\_microsoft-windows-gwx-uninstall\_31bf3856ad364e35\_6.1.7601.23  
396\_none\_0b8d69aa2b6cdb3f\GWXGC.exe  
ModTime: Sun Mar 20 14:02:02 2016 Z  
Executed

C:\Program Files\Common Files\Apple\Mobile Device  
Support\AppleMobileDeviceService.exe  
ModTime: Fri May 29 22:51:26 2015 Z  
Executed

C:\Windows\System32\unregmp2.exe  
ModTime: Tue Jul 14 01:39:48 2009 Z  
Executed

C:\WINDOWS\Installer\MSI458C.tmp  
ModTime: Tue Apr 19 20:41:20 2016 Z  
Executed

C:\Windows\System32\PhotoMetadataHandler.dll  
ModTime: Tue Jul 14 01:41:53 2009 Z

D:\install\data\Disk1\vcredist32.exe  
ModTime: Mon Sep 26 01:26:27 2011 Z

C:\Windows\System32\cleanmgr.exe  
ModTime: Tue Jul 14 01:38:59 2009 Z  
Executed

C:\WINDOWS\Installer\MSIF70C.tmp  
ModTime: Mon Apr 18 15:58:36 2016 Z  
Executed

C:\WINDOWS\system32\magnify.exe  
ModTime: Tue Jul 14 01:39:16 2009 Z

C:\Program Files\HP\HP Photosmart 7520 series\Bin\ScanToPCActivationApp.exe  
ModTime: Wed Oct 17 08:29:49 2012 Z  
Executed

## SYSTEM OUTPUT

C:\Users\Abe-Arjun Malik\Downloads\DVD43\_Plugin\_Setup\_1.0.0.6.exe  
ModTime: Sun Mar 27 20:36:06 2016 Z  
Executed

C:\WINDOWS\system32\nvsvc.exe  
ModTime: Tue Nov 4 01:04:27 2014 Z  
Executed

C:\dae0984bf92096849f7d22\SetupUtility.exe  
ModTime: Thu Mar 18 19:58:36 2010 Z  
Executed

C:\Windows\Installer\MSIC0CF.tmp  
ModTime: Thu Jan 14 16:36:32 2016 Z  
Executed

C:\ProgramData\Malwarebytes\Malwarebytes Anti-Malware\mbam-setup.exe  
ModTime: Fri Mar 25 02:12:59 2016 Z  
Executed

C:\PROGRA~1\COMMON~1\McAfee\Platform\McUICnt.exe  
ModTime: Tue Nov 3 01:06:06 2015 Z  
Executed

C:\WINDOWS\system32\taskhost.exe  
ModTime: Fri Nov 23 03:13:57 2012 Z  
Executed

C:\\_SMSTaskSequence\WDPackage\fdAscripts\CenterDesktopIcons-CM12\writeIcons.cmd  
ModTime: Sun Feb 2 12:58:35 2014 Z

C:\Program Files\Windows Media Player\wmprph.exe  
ModTime: Tue Jul 14 01:39:56 2009 Z  
Executed

C:\WINDOWS\ccmsetup\vcredist\_x86.exe  
ModTime: Tue Apr 14 06:47:08 2015 Z  
Executed

C:\Program Files\Bonjour\mDNSResponder.exe  
ModTime: Wed Aug 12 21:03:42 2015 Z  
Executed

c:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\ServiceModelReg.exe  
ModTime: Wed May 28 11:50:18 2014 Z  
Executed

## SYSTEM OUTPUT

C:\WINDOWS\system32\wermgr.exe

ModTime: Tue Jul 14 01:39:51 2009 Z

Executed

C:\Windows\SysWOW64\sc.exe

ModTime: Tue Jul 14 01:39:35 2009 Z

Executed

C:\Program Files\Microsoft Office\Office14\MAPISELL.DLL

ModTime: Wed May 16 10:49:02 2012 Z

C:\Users\Abe-Arjun

Malik\AppData\Local\Temp\{5D609291-3685-4AAC-8681-90B08AE8DB8A}\{E98A9C92-E767-475B-8BC6-8780A86DDC72}\BrDifxapi64.exe

ModTime: Thu Mar 31 19:01:22 2011 Z

Executed

C:\Users\AD\_DCC~1.NCH\AppData\Local\Temp\DMT\_Files\7z.exe

ModTime: Tue Feb 3 07:09:38 2009 Z

Executed

C:\Program Files

(x86)\McAfee\SiteAdvisor\{4CE3CA3E-4996-4920-86C7-C9FB39D679C1}\mcinst.exe

ModTime: Mon May 4 20:41:41 2015 Z

Executed

C:\Program Files (x86)\Consumer Input\Update\ConsumerInputUpdate.exe

ModTime: Sat Feb 20 01:46:11 2016 Z

Executed

C:\Program Files\WinZip\WZSHLSTB.DLL

ModTime: Mon Apr 29 21:50:00 2013 Z

C:\Program Files\WinRAR\RarExt32.dll

ModTime: Sun Dec 1 18:09:02 2013 Z

C:\Windows\system32\gpscript.exe

ModTime: Tue Jul 14 01:39:11 2009 Z

Executed

C:\WINDOWS\Installer\MSI486B.tmp

ModTime: Tue Apr 19 20:41:20 2016 Z

Executed

C:\WINDOWS\System32\SetIEInstalledDate.exe

ModTime: Tue Dec 29 19:21:35 2015 Z

Executed



## SYSTEM OUTPUT

C:\Program Files

(x86)\Google\Update\Install\{35E8C2FB-2C8D-40D9-8085-0B679A3A8056}\47.0.2526.111\_47.0.2526.106\_chrome\_updater\_3stage.exe

ModTime: Fri Jan 15 16:59:01 2016 Z

Executed

C:\Users\AD\_DCC~1.NCH\AppData\Local\Temp\DMT\_Files\USMT\rtconsole.exe

ModTime: Tue Jul 15 21:29:22 2008 Z

Executed

C:\PROGRA~1\McAfee\MSC\mcinfo.exe

ModTime: Thu Dec 3 20:15:50 2015 Z

Executed

C:\Program Files (x86)\Google\Update\1.3.29.5\GoogleUpdateWebPlugin.exe

ModTime: Thu Feb 4 14:13:21 2016 Z

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe

ModTime: Sat Apr 12 04:08:07 2014 Z

Executed

C:\Program Files (x86)\NCH Software\Switch\mp3el.exe

ModTime: Sat Feb 20 13:29:14 2016 Z

Executed

D:\CitrixReceiver.exe

ModTime: Thu Oct 22 19:03:25 2015 Z

C:\ProgramData\dell\drivers\multiplatform\_bios\_btrfstboot\x86\_64\cctk.exe

ModTime: Fri Sep 27 06:19:56 2013 Z

Executed

C:\Program Files (x86)\Microsoft Office\Office12\POWERPNT.EXE

ModTime: Fri Oct 16 23:35:38 2015 Z

Executed

C:\Users\AD\_DCC~1.NCH\AppData\Local\Temp\EnvWrapper.exe

ModTime: Thu Mar 6 18:31:23 2014 Z

Executed

C:\Windows\SoftwareDistribution\Download\Install\ndp45-kb3122656-x64.exe

ModTime: Wed Dec 16 20:07:20 2015 Z

Executed

C:\Program Files\Windows Mail\WinMail.exe

ModTime: Tue Jul 14 01:39:53 2009 Z

Executed

## SYSTEM OUTPUT

C:\Program Files\Windows Photo Viewer\ImagingDevices.exe  
ModTime: Tue Jul 14 01:43:44 2009 Z  
Executed

C:\WINDOWS\SYSTEM32\OOBE\SETUPSQM.EXE  
ModTime: Tue Jul 14 01:39:39 2009 Z  
Executed

C:\Program Files\WinZip\WINZIP64.EXE  
ModTime: Mon Apr 29 21:50:00 2013 Z  
Executed

c:\PROGRA~1\mcafee\msc\McBootSvcSet.exe  
ModTime: Tue Jan 5 15:25:16 2016 Z  
Executed

C:\WINDOWS\TEMP\mfeC300.tmp\cleanup.exe  
ModTime: Tue Jun 25 20:08:00 2013 Z  
Executed

D:\install\data\Disk1\vcredist64.exe  
ModTime: Mon Sep 26 01:26:42 2011 Z

C:\Windows\TEMP\011459~1.EXE  
ModTime: Fri Nov 27 14:49:14 2015 Z  
Executed

C:\WINDOWS\system32\igfxEM.exe  
ModTime: Thu Apr 16 19:14:55 2015 Z  
Executed

C:\WINDOWS\SoftwareDistribution\Download\Install\ndp40-kb2894842-v2-x64.exe  
ModTime: Wed Apr 15 03:30:29 2015 Z  
Executed

c:\cba99cb0f65e5bb18626ceb9\Setup.exe  
ModTime: Tue Sep 29 14:25:22 2015 Z  
Executed

C:\WINDOWS\TEMP\InstallAX\_20\_0\_0\_228.exe  
ModTime: Sun Nov 22 00:42:20 2015 Z  
Executed

C:\Program Files\WinZip\WZSHLS64.DLL  
ModTime: Mon Apr 29 21:50:00 2013 Z

C:\Program Files (x86)\McAfee\Common Framework\MfeServiceMgr.exe  
ModTime: Tue Feb 10 20:07:59 2015 Z

## SYSTEM OUTPUT

Executed

C:\Windows\Temp\{CAFECAFE-0013-0001-0122-ABCDEFABCDEF}\uncrunch.exe

ModTime: Tue Apr 5 08:38:40 2005 Z

Executed

C:\Windows\System32\SyncCenter.dll

ModTime: Sun Nov 21 03:24:51 2010 Z

C:\ProgramData\FLEXnet\Connect\11\agent.exe

ModTime: Thu Oct 13 03:11:31 2011 Z

Executed

C:\Program Files\DisplayLink Core Software\cl\_630.exe

ModTime: Mon Apr 18 15:37:28 2016 Z

Executed

C:\Windows\System32\ie4uinit.exe

ModTime: Tue Dec 29 19:21:35 2015 Z

Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\nst733C.tmp\nsissetup.exe

ModTime: Tue Jan 12 01:25:31 2016 Z

Executed

C:\Program Files\Common Files\McAfee\VSCore\_15\_4\_1\McVscIns.exe

ModTime: Thu Jan 21 21:02:18 2016 Z

Executed

C:\Users\Nikita\AppData\Local\Temp\GUMAED1.tmp\GoogleUpdateSetup.exe

ModTime: Wed Jan 13 23:13:12 2016 Z

Executed

C:\Windows\Installer\MSIE967.tmp

ModTime: Tue Feb 2 00:19:57 2016 Z

Executed

C:\WINDOWS\system32\igfxext.exe

ModTime: Thu Apr 16 19:14:55 2015 Z

Executed

C:\Program Files (x86)\Boonka\Boonka.exe

ModTime: Sat Feb 7 00:55:26 2009 Z

C:\Windows\System32\TapiUnattend.exe

ModTime: Tue Jul 14 01:39:47 2009 Z

C:\Program Files (x86)\WebEx\Document Suite\atdoced.exe

## SYSTEM OUTPUT

ModTime: Fri Sep 11 08:19:50 2015 Z  
Executed

C:\Windows\Installer\{B0119415-6743-4707-AB4D-1928F5E81FDD}\TurboTax.exe  
ModTime: Tue Jan 19 22:17:49 2016 Z

C:\Windows\System32\twext.dll  
ModTime: Sun Nov 21 03:24:16 2010 Z

C:\Users\ad\_dcc\_s.nchotu\Desktop\Launch\_PCRestore.exe  
ModTime: Mon Nov 17 16:39:10 2014 Z  
Executed

C:\Program Files\Windows Sidebar\sbdrop.dll  
ModTime: Tue Jul 14 01:41:53 2009 Z

C:\WINDOWS\WinSxS\x86\_microsoft-windows-ie-pdm\_31bf3856ad364e35\_8.0.7601.17514\_none\_0a379bcfbdcffb74\PDMSSetup.exe  
ModTime: Sun Nov 21 03:25:08 2010 Z  
Executed

C:\Program Files\Common Files\McAfee\ActWiz\mcautoreg.exe  
ModTime: Mon Dec 21 12:38:48 2015 Z  
Executed

C:\Program Files\Windows Photo Viewer\PhotoViewer.dll  
ModTime: Sun Nov 21 03:25:06 2010 Z

C:\Program Files\Microsoft Office\Office14\MSOHEVI.DLL  
ModTime: Thu Dec 13 17:48:59 2012 Z

C:\Windows\System32\prnfltr.dll  
ModTime: Sun Nov 21 03:23:48 2010 Z

C:\Program Files\Windows NT\Accessories\wordpad.exe  
ModTime: Sun Nov 21 03:24:34 2010 Z

C:\WINDOWS\system32\xcopy.exe  
ModTime: Tue Jul 14 01:14:50 2009 Z

C:\WINDOWS\syswow64\wbem\wmiprvse.exe  
ModTime: Sun Nov 21 03:24:27 2010 Z  
Executed

C:\Program Files (x86)\WIDI 4.4 Pro\Uninstall.exe  
ModTime: Sat Feb 20 02:36:48 2016 Z  
Executed

## SYSTEM OUTPUT

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\NGen.exe  
ModTime: Thu Mar 20 22:49:19 2014 Z  
Executed

C:\WINDOWS\Installer\MSI8AD8.tmp  
ModTime: Mon Apr 18 15:57:03 2016 Z  
Executed

C:\WINDOWS\system32\bcdedit.exe  
ModTime: Sun Nov 21 03:24:22 2010 Z  
Executed

C:\DMTFiles\usmt\5\X64\mighost.exe  
ModTime: Wed Jul 25 23:23:59 2012 Z  
Executed

C:\WINDOWS\Installer\MSIBD75.tmp  
ModTime: Wed Apr 20 15:00:51 2016 Z  
Executed

C:\Users\ABE-AR~1\AppData\Local\Temp\~nsu.tmp\Au\_.exe  
ModTime: Sat Feb 20 02:36:48 2016 Z  
Executed

c:\PROGRA~1\mcafee\VIRUSS~1\mcods.exe  
ModTime: Tue Oct 20 23:13:26 2015 Z  
Executed

C:\WINDOWS\TEMP\{B7D533EB-EC10-4B6C-94A4-818CBD64D2FA}\ISBEW64.exe  
ModTime: Mon Apr 18 15:57:47 2016 Z  
Executed

C:\Windows\Temp\nsk577A.tmp\FilestoInstall\PEFHelper.exe  
ModTime: Wed Mar 2 17:17:39 2016 Z  
Executed

C:\Program Files (x86)\McAfee\Common Framework\x86\policyupgrade.exe  
ModTime: Thu Sep 24 00:06:22 2015 Z  
Executed

C:\Program Files (x86)\TurboTax\Deluxe 2015\32bit\awesomium\_process  
ModTime: Wed Oct 14 12:15:07 2015 Z  
Executed

C:\Windows\Temp\{CAFECAFE-0013-0001-0126-ABCDEFABCDEF}\uncrunch.exe  
ModTime: Tue May 16 08:50:17 2006 Z  
Executed

## SYSTEM OUTPUT

C:\Program Files (x86)\Nuance\PaperPort\pplinks.exe  
 ModTime: Tue Aug 2 21:48:36 2011 Z

C:\Program Files (x86)\McAfee\SiteAdvisor\Download\s7i4.p.exe  
 ModTime: Tue Apr 5 08:30:30 2016 Z  
 Executed

-----  
 auditfail v.20081212  
 (System) Get CrashOnAuditFail value

CrashOnAuditFail = 0  
 Feature is off; the system will not halt

-----  
 backuprestore v.20130904  
 (System) Gets the contents of the FilesNotToSnapshot, KeysNotToRestore, and  
 FilesNotToBackup keys

ControlSet001\Control\BackupRestore\FilesNotToSnapshot  
 LastWrite Time Thu Sep 10 21:32:13 2015 (UTC)  
 The listed directories/files are not backed up in Volume Shadow Copies

WUA : %windir%\softwaredistribution\\*. \* /s  
 OutlookOAB : \$UserProfile\$\AppData\Local\Microsoft\Outlook\\*.oab  
 OutlookOST : \$UserProfile\$\AppData\Local\Microsoft\Outlook\\*.ost  
 FVE : \$AllVolumes\$\System Volume  
 Information\FVE.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}  
 RAC : %ProgramData%\Microsoft\RAC\\* %ProgramData%\Microsoft\RAC\StateData\\*  
 %ProgramData%\Microsoft\RAC\Outbound\\* %ProgramData%\Microsoft\RAC\PublishedData\\*  
 %ProgramData%\Microsoft\RAC\Temp\\*  
 OfficeODC :  
 \$UserProfile\$\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\\*.fsf  
 \$UserProfile\$\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\\*.fsd  
 \$UserProfile\$\Local Settings\Application Data\Office\14.0\OfficeFileCache\\*.fsd  
 \$UserProfile\$\Local Settings\Application Data\Office\14.0\OfficeFileCache\\*.fsf  
 \$UserProfile\$\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEdit  
 Manager\\*.fsf  
 \$UserProfile\$\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEdit  
 Manager\\*.fsd \$UserProfile\$\Local Settings\Application  
 Data\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\\*.fsd \$UserProfile\$\Local  
 Settings\Application  
 Data\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\\*.fsf

FilesNotToBackup key  
 ControlSet001\Control\BackupRestore\FilesNotToBackup  
 LastWrite Time Mon Dec 1 12:58:40 2014 (UTC)  
 Specifies the directories and files that backup applications should not backup or  
 restore

## SYSTEM OUTPUT

Temporary Files : %TEMP%\\* /s  
 Power Management : \hiberfil.sys  
 Memory Page File : \Pagefile.sys  
 Offline Files Cache : C:\Windows\CSC\\* /s  
 Netlogon : %SystemRoot%\netlogon.chg  
 Internet Explorer : %UserProfile%\index.dat /s  
 BITS\_LOG : C:\Windows\System32\Bits.log  
 BITS\_BAK : C:\Windows\System32\Bits.bak  
 WUA : %windir%\softwaredistribution\\*. \* /s  
 WER : %ProgramData%\Microsoft\Windows\WER\\* /s  
 BITS\_metadata : C:\ProgramData\Microsoft\Network\Downloader\  
 ETW : %SystemRoot%\system32\LogFiles\WMI\RtBackup\\*. \*  
 Kernel Dumps : %systemroot%\Minidump\\* /s %systemroot%\memory.dmp  
 Mount Manager : \System Volume Information\MountPointManagerRemoteDatabase  
 VSS Default Provider : \System Volume  
 Information\\*{3808876B-C176-4e48-B7AE-04046E6CC752} /s  
 VSS Service DB : \System Volume  
 Information\\*.{7cc467ef-6865-4831-853f-2a4817fd1bca}DB  
 FVE\_Log : \System Volume Information\FVE.{c9ca54a3-6983-46b7-8684-a7e5e23499e3}  
 FVE\_Wipe : \System Volume Information\FVE.{9ef82dfa-1239-4a30-83e6-3b3e9b8fed08}  
 VSS Service Alternate DB : \System Volume  
 Information\\*.{7cc467ef-6865-4831-853f-2a4817fd1bca}ALT  
 FVE\_Control : \System Volume  
 Information\FVE.{e40ad34d-dae9-4bc7-95bd-b16218c10f72}. \*  
 MS Distributed Transaction Coordinator : C:\Windows\system32\MSDtc\MSDTC.LOG  
 C:\Windows\system32\MSDtc\trace\dtctrace.log  
 RAC : %ProgramData%\Microsoft\RAC\\* %ProgramData%\Microsoft\RAC\StateData\  
 %ProgramData%\Microsoft\RAC\Outbound\\* %ProgramData%\Microsoft\RAC\PublishedData\  
 %ProgramData%\Microsoft\RAC\Temp\\*

KeysNotToRestore key  
 ControlSet001\Control\BackupRestore\KeysNotToRestore  
 LastWrite Time Tue Jul 14 04:49:01 2009 (UTC)

Specifies the names of the registry subkeys and values that backup applications should not restore

Mount Manager : MountedDevices\  
 MS Distributed Transaction Coordinator : CurrentControlSet\Control\MSDTC\ASR\  
 Session Manager : CurrentControlSet\Control\Session Manager\AllowProtectedRenames  
 Pending Rename Operations : CurrentControlSet\Control\Session  
 Manager\PendingFileRenameOperations  
 Pending Rename Operations2 : CurrentControlSet\Control\Session  
 Manager\PendingFileRenameOperations2

-----  
comname v.20090727

(System) Gets ComputerName and Hostname values from System hive

## SYSTEM OUTPUT

ComputerName = ABE-ARJUNMALIK  
 TCP/IP Hostname = Abe-ArjunMalik  
 -----

crashcontrol v.20131210  
 (System) Get crash control information

CrashDumpEnabled = 2 [Kernel memory dump]  
 DumpFile = %SystemRoot%\MEMORY.DMP  
 MinidumpDir = %SystemRoot%\Minidump  
 LogEvent = 1  
 Logs an event to the System Event Log (event ID = 1001, source = Save Dump)  
 -----

ddm v.20081129  
 (System) Get DDM data from Control Subkey

ControlSet001\Control\DDM not found.  
 -----

devclass v.20130630  
 (System) Get USB device info from the DeviceClasses keys in the System hive

DevClasses - Disks  
 ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Wed Apr 6 14:24:59 2016 (UTC)  
 Disk&Ven\_SanDisk&Prod\_Cruzer\_Micro&Rev\_8.02,2243400CB8E0533D&0  
 Wed Apr 6 14:20:53 2016 (UTC)  
 Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_8192,AABA1ECC00001167&0  
 Sat Mar 19 22:25:24 2016 (UTC)  
 Disk&Ven\_&Prod\_&Rev\_PMAP,070B43D9AB6E9253&0  
 Sat Mar 19 22:24:04 2016 (UTC)  
 Disk&Ven\_&Prod\_&Rev\_2.20,0718011120035AF&0  
 Thu Feb 18 16:36:21 2016 (UTC)  
 Disk&Ven\_Seagate&Prod\_FreeAgent&Rev\_0132,2GEYC3F8\_\_\_\_&0  
 Fri Jan 15 00:57:33 2016 (UTC)  
 Disk&Ven\_&Prod\_&Rev\_PMAP,07032B5A180AA664&0  
 Thu Dec 17 13:01:17 2015 (UTC)  
 Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_1100,ACB3HD1000000240&0  
 Fri Nov 20 01:55:54 2015 (UTC)  
 Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00,C68B200FB019&1  
 Fri Nov 20 01:55:53 2015 (UTC)  
 Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00,C68B200FB019&0  
 Fri Nov 20 01:55:52 2015 (UTC)  
 Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00,C68B200FB019&2  
 Thu Nov 19 17:47:57 2015 (UTC)  
 Disk&Ven\_Apple&Prod\_iPod&Rev\_2.70,000A27001CA9A995&0  
 Mon Oct 26 09:55:50 2015 (UTC)  
 Disk&Ven\_SanDisk&Prod\_Cruzer&Rev\_1.20,200544568018E7B0762E&0



## SYSTEM OUTPUT

Thu Oct 8 00:29:42 2015 (UTC)

Disk&Ven\_Seagate&Prod\_BUP\_Slim\_SL&Rev\_0302,NA76YAT8&0

Wed Oct 7 01:06:15 2015 (UTC)

Disk&Ven\_hp&Prod\_USB\_FLASH\_DRIVE&Rev\_1.00,002354D46B97AC5102CF01C0&0

Thu Oct 1 23:47:40 2015 (UTC)

Disk&Ven\_&Prod\_&Rev\_PMAP,070B43D2DE271C28&0

Fri Feb 20 17:01:42 2015 (UTC)

Disk&Ven\_SanDisk&Prod\_Cruzer&Rev\_8.02,17380302D5A10198&0

## DevClasses - Volumes

ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

Device : VID\_05AC&PID\_12A8&MI\_00

LastWrite: Thu Sep 24 18:59:56 2015 UTC

Device : VID\_091E&PID\_455B

LastWrite: Sat Sep 12 00:09:28 2015 UTC

Device : DISK&VEN\_JMCR&PROD\_SD&REV\_ SN: 5&12E35340&0&000000

LastWrite: Wed Sep 23 03:08:50 2015 UTC

Device : DISK&VEN\_&PROD\_&REV\_2.20 SN: 0718011120035AF&0

LastWrite: Mon Oct 19 13:06:21 2015 UTC

Device : DISK&VEN\_&PROD\_&REV\_PMAP SN: 07032B5A180AA664&0

LastWrite: Mon Sep 14 18:39:11 2015 UTC

Device : DISK&VEN\_&PROD\_&REV\_PMAP SN: 070B43D2DE271C28&0

LastWrite: Thu Oct 1 23:47:49 2015 UTC

Device : DISK&VEN\_&PROD\_&REV\_PMAP SN: 070B43D9AB6E9253&0

LastWrite: Sat Mar 19 22:25:27 2016 UTC

Device : DISK&VEN\_APPLE&PROD\_IPOD&REV\_2.70 SN: 000A27001CA9A995&0

LastWrite: Thu Nov 19 17:48:07 2015 UTC

Device : DISK&VEN\_HP&PROD\_USB\_FLASH\_DRIVE&REV\_1.00 SN: 002354D46B97AC5102CF01C0&0

LastWrite: Sat Sep 12 01:43:29 2015 UTC

Device : DISK&VEN\_PNY&PROD\_USB\_2.0\_FD&REV\_1100 SN: ACB3HD1000000240&0

LastWrite: Thu Oct 8 00:18:01 2015 UTC

Device : DISK&VEN\_PNY&PROD\_USB\_2.0\_FD&REV\_8192 SN: AABA1ECC00001167&0

LastWrite: Mon Oct 19 13:06:32 2015 UTC

Device : DISK&VEN\_SANDISK&PROD\_CRUZER&REV\_1.20 SN: 200544568018E7B0762E&0

LastWrite: Mon Oct 26 09:56:12 2015 UTC

## SYSTEM OUTPUT

Device : DISK&VEN\_SANDISK&PROD\_CRUZER&REV\_8.02 SN: 17380302D5A10198&0  
 LastWrite: Fri Feb 20 17:01:44 2015 UTC

Device : DISK&VEN\_SANDISK&PROD\_CRUZER\_MICRO&REV\_8.02 SN: 2243400CB8E0533D&0  
 LastWrite: Wed Apr 6 14:25:07 2016 UTC

Device : DISK&VEN\_SONY&PROD\_DSC&REV\_1.00 SN: C68B200FB019&0  
 LastWrite: Fri Nov 20 01:55:59 2015 UTC

Device : DISK&VEN\_SONY&PROD\_DSC&REV\_1.00 SN: C68B200FB019&1  
 LastWrite: Fri Nov 20 01:56:02 2015 UTC

Device : DISK&VEN\_SONY&PROD\_DSC&REV\_1.00 SN: C68B200FB019&2  
 LastWrite: Fri Nov 20 01:55:58 2015 UTC

-----  
 disablelastaccess v.20090118  
 (System) Get NTFSDisableLastAccessUpdate value

NtfsDisableLastAccessUpdate  
 ControlSet001\Control\FileSystem  
 NtfsDisableLastAccessUpdate = 1  
 -----

dllsearch v.20100824  
 (System) Get crash control information

dllsearch v.20100824

CWDIllegalInDllSearch value not found.  
 -----

eventlog v.20090112  
 (System) Get EventLog configuration info

Application \ Wed Feb 10 01:13:33 2016Z

File = %SystemRoot%\system32\winevt\Logs\Application.evtx  
 DisplayNameFile = %SystemRoot%\system32\wevtapi.dll  
 MaxSize = 20.00MB  
 Retention = 0 sec  
 AutoBackupLogFiles = 0

HardwareEvents \ Tue Jul 14 04:49:01 2009Z

File = %systemroot%\system32\winevt\logs\HardwareEvents.evtx  
 DisplayNameFile = %SystemRoot%\system32\wecsvc.dll  
 MaxSize = 20.00MB  
 Retention = 0 sec

Internet Explorer \ Tue Jul 14 04:49:01 2009Z

## SYSTEM OUTPUT

Key Management Service \ Tue Jul 14 04:49:01 2009Z

MaxSize = 20.00MB  
Retention = 0 sec

Media Center \ Tue Apr 12 08:28:45 2011Z

File = %SystemRoot%\System32\winevt\Logs\Media Center.evtx  
MaxSize = 8.00MB  
Retention = 0 sec

OAlerts \ Thu Sep 10 21:32:12 2015Z

DisplayNameFile = C:\PROGRA~2\COMMON~1\MICROS~1\OFFICE14\OFFREL.DLL  
MaxSize = 128.00KB  
Retention = 0 sec

ODiag \ Thu Sep 10 16:33:31 2015Z

DisplayNameFile = C:\PROGRA~2\COMMON~1\MICROS~1\OFFICE12\OFFREL.DLL  
MaxSize = 16.00MB  
Retention = 0 sec

OSession \ Thu Sep 10 16:33:31 2015Z

DisplayNameFile = C:\PROGRA~2\COMMON~1\MICROS~1\OFFICE12\OFFREL.DLL  
MaxSize = 16.00MB  
Retention = 0 sec

Security \ Thu Sep 10 21:48:06 2015Z

File = %SystemRoot%\System32\winevt\Logs\Security.evtx  
DisplayNameFile = %SystemRoot%\system32\wevtapi.dll  
MaxSize = 20.00MB  
Retention = 0 sec

System \ Wed Apr 13 11:43:17 2016Z

File = %SystemRoot%\system32\winevt\Logs\System.evtx  
DisplayNameFile = %SystemRoot%\system32\wevtapi.dll  
MaxSize = 20.00MB  
Retention = 0 sec

Windows PowerShell \ Tue Jul 14 04:49:01 2009Z

MaxSize = 15.00MB  
Retention = 0 sec  
AutoBackupLogFiles = 0

-----  
eventlogs v.20081219

(System) Gets Event Log settings from System hive

EventLog Configuration

ControlSet001\Services\Eventlog

## SYSTEM OUTPUT

LastWrite Time Thu Sep 10 21:30:14 2015 (UTC)

-----

fw\_config v.20080328

(System) Gets the Windows Firewall config from the System hive

Windows Firewall Configuration

ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile

LastWrite Time Sun Nov 21 03:57:14 2010 (UTC)

EnableFirewall -> 1

DisableNotifications -> 0

Windows Firewall Configuration

ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile

LastWrite Time Sun Nov 21 03:57:14 2010 (UTC)

EnableFirewall -> 1

DisableNotifications -> 0

-----

hibernate v.20081216

(System) Check hibernation status

Error reading Heuristics value.

-----

ide v.20080418

(System) Get IDE device info from the System hive file

IDE

ControlSet001\Enum\IDE

LastWrite Time Mon Apr 18 00:13:48 2016 (UTC)

CdRomhp\_DVD RAM\_GT50N\_\_\_\_\_MP00\_\_\_\_\_ [Mon Apr 18 00:13:48 2016]

5&2f70901&0&1.0.0 [Wed Apr 20 02:36:34 2016 (UTC)]

FriendlyName : hp DVD RAM GT50N ATA Device

CdRomhp\_DVD A\_DS8A8SH\_\_\_\_\_KH61\_\_\_\_\_ [Mon Apr 18 00:13:48 2016]

5&2f70901&0&1.0.0 [Mon Apr 18 00:13:48 2016 (UTC)]

FriendlyName : hp DVD A DS8A8SH ATA Device

CdRomhp\_DVD D\_DS8D3SH\_\_\_\_\_HH61\_\_\_\_\_ [Mon Apr 18 00:13:48 2016]

5&2f70901&0&1.0.0 [Mon Apr 18 00:13:48 2016 (UTC)]

FriendlyName : hp DVD D DS8D3SH ATA Device

DiskHitachi\_HTS723232A7A364\_\_\_\_\_EC20A60W [Mon Apr 18 00:13:48 2016]

5&2bd82263&0&0.0.0 [Wed Apr 20 02:36:34 2016 (UTC)]

FriendlyName : Hitachi HTS723232A7A364 ATA Device

## SYSTEM OUTPUT

DiskSAMSUNG\_MZ7PC128HAFU-000H1\_\_\_\_\_CXM05H1Q [Mon Apr 18 00:13:48 2016]  
 5&2bd82263&0&0.0.0 [Mon Apr 18 00:13:48 2016 (UTC)]  
 FriendlyName : SAMSUNG MZ7PC128HAFU-000H1 ATA Device

DevClasses - Disks

ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Wed Apr 20 02:36:34 2016 (UTC)

DiskHitachi\_HTS723232A7A364\_\_\_\_\_EC20A60W, 5&2bd82263&0&0.0.0

Fri Feb 20 18:43:28 2015 (UTC)

DiskSAMSUNG\_MZ7PC128HAFU-000H1\_\_\_\_\_CXM05H1Q, 5&2bd82263&0&0.0.0

-----  
 imagedev v.20140104

(System) --

imagedev

ControlSet001\Control\Class\{6BDD1FC6-810F-11D0-BEC7-08002BE2092F}

Still Image Capture Devices

-----  
 kbdcrash v.20081212

(System) Checks to see if system is config to crash via keyboard

CrashOnCtrlScroll not set

-----  
 legacy v.20120524

(System) Lists LEGACY\_\* entries in Enum\Root key

Wed Apr 20 02:37:11 2016 (UTC)

LEGACY\_MBAMWEBACCESSCONTROL\0000 - MBAMWebAccessControl

Wed Apr 20 02:37:02 2016 (UTC)

LEGACY\_SRV\0000 - @%systemroot%\system32\svcsvc.dll, -102

LEGACY\_SRV2\0000 - @%systemroot%\system32\svcsvc.dll, -104

LEGACY\_SRVNET\0000 - srvnet

Wed Apr 20 02:36:56 2016 (UTC)

LEGACY\_BOWSER\0000 - @%systemroot%\system32\browser.dll, -102

LEGACY\_MRXSMB\0000 - @%systemroot%\system32\wkssvc.dll, -1002

LEGACY\_MRXSMB10\0000 - @%systemroot%\system32\wkssvc.dll, -1004

LEGACY\_MRXSMB20\0000 - @%systemroot%\system32\wkssvc.dll, -1006

Wed Apr 20 02:36:51 2016 (UTC)

LEGACY\_LUAFV\0000 - @%systemroot%\system32\drivers\luafv.sys, -100

LEGACY\_MBAMPROTECTOR\0000 - MBAMProtector

Wed Apr 20 02:36:38 2016 (UTC)

LEGACY\_DFSC\0000 - @%systemroot%\system32\drivers\dfsc.sys, -101

LEGACY\_MSFS\0000 - Msfs

LEGACY\_NETBIOS\0000 - NetBIOS Interface

## SYSTEM OUTPUT

LEGACY\_NPFS\0000 - Npfs  
 LEGACY\_RDBSS\0000 - @%systemroot%\system32\wkssvc.dll,-1000  
 Wed Apr 20 02:36:34 2016 (UTC)  
 LEGACY\_FILEINFO\0000 - @%SystemRoot%\system32\drivers\fileinfo.sys,-100  
 LEGACY\_FLTMGR\0000 - @%SystemRoot%\system32\drivers\fltMgr.sys,-10001  
 LEGACY\_FS\_REC\0000 - Fs\_Rec  
 LEGACY\_MUP\0000 - @%systemroot%\system32\drivers\mup.sys,-101  
 LEGACY\_NTFS\0000 - Ntfs  
 Wed Apr 20 02:36:33 2016 (UTC)  
 LEGACY\_AFD\0000 - @%systemroot%\system32\drivers\afd.sys,-1000  
 LEGACY\_AMDKMDAG\0000 - amdKMDag  
 LEGACY\_AMDKMPFD\0000 - AMD PCI Root Bus Lower Filter  
 LEGACY\_ATAPI\0000 - IDE Channel  
 LEGACY\_BEEP\0000 - Beep  
 LEGACY\_CFWIDS\0000 - McAfee Inc. cfwids  
 LEGACY\_CLFS\0000 - @%SystemRoot%\system32\clfs.sys,-100  
 LEGACY\_CNG\0000 - CNG  
 LEGACY\_CSC\0000 - @%systemroot%\system32\csccvc.dll,-202  
 LEGACY\_DISCACHE\0000 - @%systemroot%\system32\drivers\discache.sys,-102  
 LEGACY\_DXGKRNL\0000 - LDDM Graphics Subsystem  
 LEGACY\_FVEVOL\0000 - @%SystemRoot%\system32\drivers\fvevol.sys,-100  
 LEGACY\_HTTP\0000 - @%SystemRoot%\system32\drivers\http.sys,-1  
 LEGACY\_HWPOLICY\0000 - @%systemroot%\system32\drivers\hwpolicy.sys,-101  
 LEGACY\_KSECDD\0000 - KSecDD  
 LEGACY\_KSECPKG\0000 - KSecPkg  
 LEGACY\_LLTDIO\0000 - Link-Layer Topology Discovery Mapper I/O Driver  
 LEGACY\_MFEAACK\0000 - McAfee Inc. mfeaack  
 LEGACY\_MFEAVFK\0000 - McAfee Inc. mfeavfk  
 LEGACY\_MFEFIREK\0000 - McAfee Inc. mfefirek  
 LEGACY\_MFEHIDK\0000 - McAfee Inc. mfehik  
 LEGACY\_MFENCBCD\0000 - McAfee Inc. mfencbcd  
 LEGACY\_MFENCRK\0000 - McAfee Inc. mfencrk  
 LEGACY\_MFESAPSN\0000 - McAfee Process Start Notification Service  
 LEGACY\_MFEWFPK\0000 - McAfee Inc. mfewfpk  
 LEGACY\_MOUNTMGR\0000 - @%SystemRoot%\system32\drivers\mountmgr.sys,-100  
 LEGACY\_MPSPDRV\0000 - @%SystemRoot%\system32\FirewallAPI.dll,-23092  
 LEGACY\_MSISADRV\0000 - msisadrv  
 LEGACY\_NATIVEWIFI\0000 - NativeWiFi Filter  
 LEGACY\_NDIS\0000 - @%SystemRoot%\system32\drivers\ndis.sys,-200  
 LEGACY\_NDISUIO\0000 - NDIS Usermode I/O Protocol  
 LEGACY\_NDPROXY\0000 - NDProxy  
 LEGACY\_NETBT\0000 - @%SystemRoot%\system32\drivers\netbt.sys,-2  
 LEGACY\_NSIPROXY\0000 - @%SystemRoot%\system32\drivers\nsiproxy.sys,-2  
 LEGACY\_NULL\0000 - Null  
 LEGACY\_PCW\0000 - Performance Counters for Windows Driver  
 LEGACY\_PEAUTH\0000 - PEAUTH  
 LEGACY\_PSCHEDE\0000 - @%SystemRoot%\System32\drivers\pacer.sys,-101  
 LEGACY\_RDPCDD\0000 - @%systemroot%\system32\DRIVERS\RDPCDD.sys,-100

## SYSTEM OUTPUT

LEGACY\_RDPENCDD\0000 - @%systemroot%\system32\drivers\RDPEncdd.sys,-101  
 LEGACY\_RDPREFMP\0000 - @%systemroot%\system32\drivers\RdpRefMp.sys,-101  
 LEGACY\_RSPNDR\0000 - Link-Layer Topology Discovery Responder  
 LEGACY\_SECDRV\0000 - Security Driver  
 LEGACY\_SPLDR\0000 - Security Processor Loader Driver  
 LEGACY\_STORFLT\0000 - @%SystemRoot%\system32\vmstorfltres.dll,-1000  
 LEGACY\_TCPIP\0000 - @%SystemRoot%\system32\tcpipcfg.dll,-50003  
 LEGACY\_TCPIPREG\0000 - TCP/IP Registry Compatibility  
 LEGACY\_TDX\0000 - @%SystemRoot%\system32\tcpipcfg.dll,-50004  
 LEGACY\_VGASAVE\0000 - VgaSave  
 LEGACY\_VOLMGRX\0000 - @%SystemRoot%\system32\drivers\volmgrx.sys,-100  
 LEGACY\_VOLSNAP\0000 - Storage volumes  
 LEGACY\_VWIFIFLT\0000 - Virtual WiFi Filter Driver  
 LEGACY\_WANARPV6\0000 - @%systemroot%\system32\rascfg.dll,-32012  
 LEGACY\_WDF01000\0000 - @%SystemRoot%\system32\drivers\Wdf01000.sys,-1000  
 LEGACY\_WFPLWF\0000 - WFP Lightweight Filter  
 LEGACY\_WS2IFSL\0000 - Windows Socket 2.0 Non-IFS Service Provider Support Environment  
 LEGACY\_WUDFPF\0000 - @%SystemRoot%\system32\drivers\Wudfpf.sys,-1000  
 Wed Apr 20 02:31:57 2016 (UTC)  
 LEGACY\_MBAMSWISSARMY  
 LEGACY\_MBAMSWISSARMY\0000 - MBAMSwissArmy  
 Mon Apr 18 00:13:48 2016 (UTC)  
 LEGACY\_AFD  
 LEGACY\_AMDKMDAG  
 LEGACY\_AMDKMPFD  
 LEGACY\_ATAPI  
 LEGACY\_BEEP  
 LEGACY\_BOWSER  
 LEGACY\_CDFS  
 LEGACY\_CDFS\0000 - CD/DVD File System Reader  
 LEGACY\_CFWIDS  
 LEGACY\_CLFS  
 LEGACY\_CNG  
 LEGACY\_CSC  
 LEGACY\_DFSC  
 LEGACY\_DISCACHE  
 LEGACY\_DXGKRNL  
 LEGACY\_EXFAT  
 LEGACY\_EXFAT\0000 - exFAT File System Driver  
 LEGACY\_FASTFAT  
 LEGACY\_FASTFAT\0000 - FAT12/16/32 File System Driver  
 LEGACY\_FILEINFO  
 LEGACY\_FLTMGR  
 LEGACY\_FS\_REC  
 LEGACY\_FVEVOL  
 LEGACY\_HTTP  
 LEGACY\_HWPOLICY

## SYSTEM OUTPUT

LEGACY\_KSECDD  
LEGACY\_KSECPKG  
LEGACY\_LLTDIO  
LEGACY\_LUAFV  
LEGACY\_MBAMPROTECTOR  
LEGACY\_MBAMWEBACCESSCONTROL  
LEGACY\_MFEAACK  
LEGACY\_MFEAACK01  
LEGACY\_MFEAACK01\0000 - McAfee Inc.  
LEGACY\_MFEAVFK  
LEGACY\_MFEAVFK01  
LEGACY\_MFEAVFK01\0000 - McAfee Inc.  
LEGACY\_MFEFIREK  
LEGACY\_MFEHIDK  
LEGACY\_MFEHIDK01  
LEGACY\_MFEHIDK01\0000 - McAfee Inc.  
LEGACY\_MFENCBDC  
LEGACY\_MFENCRK  
LEGACY\_MFESAPSN  
LEGACY\_MFEWFPK  
LEGACY\_MOUNTMGR  
LEGACY\_MPSPDRV  
LEGACY\_MRXSMB  
LEGACY\_MRXSMB10  
LEGACY\_MRXSMB20  
LEGACY\_MSFS  
LEGACY\_MSISADRV  
LEGACY\_MUP  
LEGACY\_NATIVEWIFIP  
LEGACY\_NDIS  
LEGACY\_NDISUIO  
LEGACY\_NDPROXY  
LEGACY\_NETBIOS  
LEGACY\_NETBT  
LEGACY\_NPFS  
LEGACY\_NSIPROXY  
LEGACY\_NTFS  
LEGACY\_NULL  
LEGACY\_PCW  
LEGACY\_PEAUTH  
LEGACY\_PSCHED  
LEGACY\_RDBSS  
LEGACY\_RDPDCC  
LEGACY\_RDPENCDD  
LEGACY\_RDPREFMP  
LEGACY\_RSPNDR  
LEGACY\_SECDRV  
LEGACY\_SPLDR



## SYSTEM OUTPUT

```

LEGACY_SRV
LEGACY_SRV2
LEGACY_SRVNET
LEGACY_STORFLT
LEGACY_TCPIP
LEGACY_TCPIPREG
LEGACY_TDX
LEGACY_UDFS
LEGACY_UDFS\0000 - udfs
LEGACY_VGASAVE
LEGACY_VOLMGRX
LEGACY_VOLSnap
LEGACY_VWIFIFLT
LEGACY_WANARPV6
LEGACY_WDF01000
LEGACY_WFPLWF
LEGACY_WIMMOUNT
LEGACY_WIMMOUNT\0000 - WIMMount
LEGACY_WS2IFSL
LEGACY_WUDFPF

```

-----  
mountdev v.20130530

(System) Return contents of System hive MountedDevices key

MountedDevices

LastWrite time = Wed Apr 6 14:25:01 2016Z

```

\??\Volume{2c8d8b43-b930-11e4-820a-806e6f6e6963}
  Drive Signature = 60 a4 b8 5c
\??\Volume{2c8d8b44-b930-11e4-820a-806e6f6e6963}
  Drive Signature = 60 a4 b8 5c
\??\Volume{2c8d8b45-b930-11e4-820a-806e6f6e6963}
  Drive Signature = 60 a4 b8 5c
\DosDevices\C:
  Drive Signature = 60 a4 b8 5c
\??\Volume{fd9f8cc4-5263-11e5-b0ce-806e6f6e6963}
  Drive Signature = 60 a4 b8 5c
\??\Volume{a5294079-57dd-11e5-a189-402cf486a5d9}
  Drive Signature = 99 ec ad 3c
\DosDevices\G:
  Drive Signature = c6 aa 4b 6d
\??\Volume{c0e9ffaf-960c-11e5-ac0f-402cf486a5d9}
  Drive Signature = c6 aa 4b 6d

```

Device:

```

_??_USBSTOR#Disk&Ven_&Prod_&Rev_2.20#0718011120035AF&0#{53f56307-b6bf-11d0-94f2-00a0
c91efb8b}

```

## SYSTEM OUTPUT

\\?\Volume{0835c2e6-61a2-11e5-8066-402cf486a5d9}

## Device:

\_?\_USBSTOR#Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_1100#ACB3HD1000000240&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

\\?\Volume{0835bd53-61a2-11e5-8066-402cf486a5d9}

## Device:

\_?\_USBSTOR#Disk&Ven\_SanDisk&Prod\_Cruzer&Rev\_1.20#200544568018E7B0762E&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

\\?\Volume{9a16e661-776d-11e5-8f09-402cf486a5d9}

## Device:

\_?\_USBSTOR#Disk&Ven\_hp&Prod\_USB\_FLASH\_DRIVE&Rev\_1.00#002354D46B97AC5102CF01C0&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

\\?\Volume{26bbbfe1-58ed-11e5-964f-402cf486a5d9}

## Device:

\_?\_USBSTOR#Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00#C68B200FB019&2#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

\\?\Volume{e2ab9109-8adc-11e5-92d4-402cf486a5d9}

## Device:

\_?\_USBSTOR#Disk&Ven\_&Prod\_&Rev\_PMAP#070B43D9AB6E9253&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

\\?\Volume{4920ddd7-eae4-11e5-ae3-402cf486a5d9}

## Device:

\_?\_USBSTOR#Disk&Ven\_Apple&Prod\_iPod&Rev\_2.70#000A27001CA9A995&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

\\?\Volume{e2ab906f-8adc-11e5-92d4-402cf486a5d9}

\\DosDevices\I:

## Device:

\\?\IDE#CdRomhp\_DVDROM\_GT50N\_\_\_\_\_MP00\_\_\_\_#5&2f70901&0&1.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

\\DosDevices\D:

\\?\Volume{fd9f8ccf-5263-11e5-b0ce-806e6f6e6963}

## Device:

\_?\_USBSTOR#Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00#C68B200FB019&1#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

\\?\Volume{e2ab910f-8adc-11e5-92d4-402cf486a5d9}

\\DosDevices\H:

## Device:

\_?\_USBSTOR#Disk&Ven\_SanDisk&Prod\_Cruzer\_Micro&Rev\_8.02#2243400CB8E0533D&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

## SYSTEM OUTPUT

\DosDevices\F:

\??\Volume{a7deeca1-fb8e-11e5-836b-402cf486a5d9}

Device:

\_??\_SCSI#Disk&Ven\_JMCR&Prod\_SD&Rev\_#5&12e35340&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

\??\Volume{19b141a9-59a6-11e5-a332-402cf486a5d9}

Device:

\_??\_USBSTOR#Disk&Ven\_HP&Prod\_Photosmart\_7520&Rev\_1.00#8&2fc8d709&0&CN281291V605XX&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

\??\Volume{19b13c16-59a6-11e5-a332-402cf486a5d9}

Device:

\_??\_USBSTOR#Disk&Ven\_&Prod\_&Rev\_PMAP#07032B5A180AA664&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

\??\Volume{19b13ae2-59a6-11e5-a332-402cf486a5d9}

Device:

\_??\_USBSTOR#Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00#C68B200FB019&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

\??\Volume{e2ab910d-8adc-11e5-92d4-402cf486a5d9}

Device:

\??\IDE#CdRomhp\_DVD\_D\_DS8D3SH\_\_\_\_\_HH61\_\_\_\_\_#5&2f70901&0&1.0.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

\??\Volume{2c8d8b49-b930-11e4-820a-806e6f6e6963}

Device:

\_??\_USBSTOR#Disk&Ven\_&Prod\_&Rev\_PMAP#070B43D2DE271C28&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

\??\Volume{0835b718-61a2-11e5-8066-402cf486a5d9}

Device:

\_??\_USBSTOR#Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_8192#AABA1ECC00001167&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

\DosDevices\E:

\??\Volume{0835c2ed-61a2-11e5-8066-402cf486a5d9}

-----  
network v.20080324

(System) Gets info from System\Control\Network GUIDs

Network key

ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}

Interface {0EC4CE54-B9CF-4648-B725-D80D4E768A27}

LastWrite time Wed Apr 20 02:37:27 2016 (UTC)

Name = isatap.{3ED9F155-8201-430C-85E1-EDD7020DE0CF}

## SYSTEM OUTPUT

PnpInstanceID =  
MediaSubType =

Interface {1BDD94C3-9D85-46F0-87E3-BD3288A5F6BD}

LastWrite time Sat Nov 28 20:21:44 2015 (UTC)

Name = Local Area Connection 2  
PnpInstanceID = USB\VID\_05AC&PID\_12A8&MI\_02\2  
MediaSubType =

Interface {29898C9D-B0A4-4FEF-BDB6-57A562022CEE}

LastWrite time Sun Nov 21 03:39:55 2010 (UTC)

Name = Local Area Connection\* 2  
PnpInstanceID =  
MediaSubType =

Interface {2CAA64ED-BAA3-4473-B637-DEC65A14C8AA}

LastWrite time Tue Jul 14 04:53:20 2009 (UTC)

Name = Local Area Connection\* 8  
PnpInstanceID =  
MediaSubType =

Interface {34B9BEA8-439A-483C-A0DD-0D0F07D54445}

LastWrite time Fri Sep 11 18:23:44 2015 (UTC)

Name = Local Area Connection\* 11  
PnpInstanceID =  
MediaSubType =

Interface {3E96A3FE-0948-4CF1-B003-0E12AEFCA257}

LastWrite time Fri Feb 20 16:54:14 2015 (UTC)

Name = Local Area Connection\* 9  
PnpInstanceID =  
MediaSubType =

Interface {3ED9F155-8201-430C-85E1-EDD7020DE0CF}

LastWrite time Fri Feb 20 16:54:57 2015 (UTC)

Name = Bluetooth Network Connection  
PnpInstanceID = BTH\MS\_BTHPAN\7&2CB8892B&0&2  
MediaSubType = 7

Interface {4A853EBA-2103-43A4-99C2-A5EF5E844243}

LastWrite time Wed Apr 20 02:37:21 2016 (UTC)

Name = isatap.{A9E50A43-973B-4CAD-B78E-EA0321A4A293}  
PnpInstanceID =  
MediaSubType =

Interface {5BF54C7E-91DA-457D-80BF-333677D7E316}

LastWrite time Tue Jul 14 04:49:33 2009 (UTC)

Name = Local Area Connection\* 7

## SYSTEM OUTPUT

PnpInstanceID =  
MediaSubType =

Interface {71F897D7-EB7C-4D8D-89DB-AC80D9DD2270}  
LastWrite time Tue Jul 14 04:49:27 2009 (UTC)  
Name = Local Area Connection\*  
PnpInstanceID =  
MediaSubType =

Interface {720B974A-3E6B-42BF-9839-4EE6CD676477}  
LastWrite time Thu Sep 3 17:49:38 2015 (UTC)  
Name = Wireless Network Connection 3  
PnpInstanceID =  
PCI\VEN\_8086&DEV\_4238&SUBSYS\_11118086&REV\_3E\247703FFFF42223400  
MediaSubType = 2

Interface {73298754-907A-49BC-9D95-9603C7E27B44}  
LastWrite time Thu Jan 14 16:59:30 2016 (UTC)  
Name = Local Area Connection\* 12  
PnpInstanceID =  
MediaSubType =

Interface {749B2830-EBF4-4268-8BFD-189D3224ACFB}  
LastWrite time Fri Feb 20 16:54:57 2015 (UTC)  
Name = Local Area Connection  
PnpInstanceID =  
PCI\VEN\_8086&DEV\_1502&SUBSYS\_161C103C&REV\_04\3&E89B380&0&C8  
MediaSubType =

Interface {78032B7E-4968-42D3-9F37-287EA86C0AAA}  
LastWrite time Tue Jul 14 05:09:03 2009 (UTC)  
Name = Local Area Connection\* 10  
PnpInstanceID =  
MediaSubType =

Interface {7BAA9D10-D83A-4614-BBC4-5F7AC025E6A1}  
LastWrite time Wed Apr 20 02:37:24 2016 (UTC)  
Name = isatap.{720B974A-3E6B-42BF-9839-4EE6CD676477}  
PnpInstanceID =  
MediaSubType =

Interface {8B32CCEF-F092-453D-A04B-084246668014}  
LastWrite time Fri Feb 20 16:54:57 2015 (UTC)  
Name = Wireless Network Connection  
PnpInstanceID =  
PCI\VEN\_8086&DEV\_0085&SUBSYS\_13118086&REV\_34\8C705AFFFF220CB000  
MediaSubType = 2

## SYSTEM OUTPUT

Interface {8E301A52-AFFA-4F49-B9CA-C79096A1A056}

LastWrite time Tue Jul 14 04:49:32 2009 (UTC)

Name = Local Area Connection\* 5  
 PnpInstanceID =  
 MediaSubType =

Interface {9A399D81-2EAD-4F23-BCDD-637FC13DCD51}

LastWrite time Tue Jul 14 04:49:32 2009 (UTC)

Name = Local Area Connection\* 6  
 PnpInstanceID =  
 MediaSubType =

Interface {A9E50A43-973B-4CAD-B78E-EA0321A4A293}

LastWrite time Wed Nov 11 20:31:51 2015 (UTC)

Name = Wireless Network Connection 4  
 PnpInstanceID =  
 {5D624F94-8850-40C3-A3FA-A4FD2080BAF3}\VWIFIMP\5&114483C6&0&01  
 MediaSubType = 2

Interface {D60F25AE-ABCA-4464-AEE0-FA138E10279C}

LastWrite time Thu Sep 10 17:03:39 2015 (UTC)

Name = Local Area Connection\* 14  
 PnpInstanceID =  
 MediaSubType =

Interface {DF4A9D2C-8742-4EB1-8703-D395C4183F33}

LastWrite time Tue Jul 14 04:49:31 2009 (UTC)

Name = Local Area Connection\* 4  
 PnpInstanceID =  
 MediaSubType =

Interface {E43D242B-9EAB-4626-A952-46649FBB939A}

LastWrite time Tue Jul 14 04:49:30 2009 (UTC)

Name = Local Area Connection\* 3  
 PnpInstanceID =  
 MediaSubType =

Interface {F5100C24-B99F-4C5E-B013-9A39395D0A36}

LastWrite time Wed Apr 20 09:07:15 2016 (UTC)

Name = Reusable ISATAP Interface  
 {F5100C24-B99F-4C5E-B013-9A39395D0A36}  
 PnpInstanceID =  
 MediaSubType =

Interface {FD2B5103-617C-4AE6-8DC4-A4772C463DDC}

LastWrite time Fri Feb 20 18:22:37 2015 (UTC)

Name = Wireless Network Connection 2  
 PnpInstanceID =

## SYSTEM OUTPUT

PCI\VEN\_8086&DEV\_0085&SUBSYS\_13118086&REV\_34\606720FFFF6E81F400  
MediaSubType = 2

-----  
nic v.20100401

(System) Gets NIC info from System hive

Adapter: {1BDD94C3-9D85-46F0-87E3-BD3288A5F6BD}  
LastWrite Time: Sat Nov 28 20:21:16 2015 Z  
EnabledDHCP 1

Adapter: {3ED9F155-8201-430C-85E1-EDD7020DE0CF}  
LastWrite Time: Fri Feb 20 16:54:14 2015 Z  
EnabledDHCP 1

Adapter: {720B974A-3E6B-42BF-9839-4EE6CD676477}  
LastWrite Time: Thu Sep 3 17:49:37 2015 Z  
EnabledDHCP 1

Adapter: {749B2830-EBF4-4268-8BFD-189D3224ACFB}  
LastWrite Time: Fri Feb 20 16:53:43 2015 Z  
EnabledDHCP 1

Adapter: {8B32CCEF-F092-453D-A04B-084246668014}  
LastWrite Time: Fri Feb 20 16:53:49 2015 Z  
EnabledDHCP 1

Adapter: {A9E50A43-973B-4CAD-B78E-EA0321A4A293}  
LastWrite Time: Wed Nov 11 20:31:50 2015 Z  
EnabledDHCP 1

Adapter: {FD2B5103-617C-4AE6-8DC4-A4772C463DDC}  
LastWrite Time: Fri Feb 20 18:22:35 2015 Z  
EnabledDHCP 1

-----  
nic\_mst2 v.20080324

(System) Gets NICs from System hive; looks for MediaType = 2

Network key

ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}

ControlSet001\Services\Tcpip\Parameters\Interfaces

LastWrite time Thu Feb 18 16:19:53 2016 (UTC)

Interface {A9E50A43-973B-4CAD-B78E-EA0321A4A293}

Name: Wireless Network Connection 4

Control\Network key LastWrite time Wed Nov 11 20:31:51 2015 (UTC)

## SYSTEM OUTPUT

Services\Tcpip key LastWrite time Wed Nov 11 20:31:51 2015 (UTC)

DhcpDomain =  
 DhcpIPAddress = 0.0.0.0  
 DhcpSubnetMask = 255.0.0.0  
 DhcpNameServer =  
 DhcpServer = 255.255.255.255

Interface {FD2B5103-617C-4AE6-8DC4-A4772C463DDC}

Name: Wireless Network Connection 2

Control\Network key LastWrite time Fri Feb 20 18:22:37 2015 (UTC)

Services\Tcpip key LastWrite time Fri Feb 20 18:22:36 2015 (UTC)

DhcpDomain =  
 DhcpIPAddress = 0.0.0.0  
 DhcpSubnetMask = 255.0.0.0  
 DhcpNameServer =  
 DhcpServer = 255.255.255.255

Interface {749B2830-EBF4-4268-8BFD-189D3224ACFB}

Name: Local Area Connection

Control\Network key LastWrite time Fri Feb 20 16:54:57 2015 (UTC)

Services\Tcpip key LastWrite time Wed Apr 20 09:07:03 2016 (UTC)

DhcpDomain =  
 DhcpIPAddress = 192.168.1.179  
 DhcpSubnetMask = 255.255.255.0  
 DhcpNameServer = 192.168.1.1  
 DhcpServer = 192.168.1.1

Interface {1BDD94C3-9D85-46F0-87E3-BD3288A5F6BD}

Name: Local Area Connection 2

Control\Network key LastWrite time Sat Nov 28 20:21:44 2015 (UTC)

Services\Tcpip key LastWrite time Sun Mar 13 00:22:58 2016 (UTC)

DhcpDomain =  
 DhcpIPAddress = 172.20.10.5  
 DhcpSubnetMask = 255.255.255.240  
 DhcpNameServer = 172.20.10.1  
 DhcpServer = 172.20.10.1

Interface {3ED9F155-8201-430C-85E1-EDD7020DE0CF}

Name: Bluetooth Network Connection

Control\Network key LastWrite time Fri Feb 20 16:54:57 2015 (UTC)

Services\Tcpip key LastWrite time Fri Feb 20 16:54:14 2015 (UTC)

DhcpDomain =  
 DhcpIPAddress = 0.0.0.0  
 DhcpSubnetMask = 255.0.0.0  
 DhcpNameServer =  
 DhcpServer = 255.255.255.255

Interface {720B974A-3E6B-42BF-9839-4EE6CD676477}



## SYSTEM OUTPUT

Name: Wireless Network Connection 3

Control\Network key LastWrite time Thu Sep 3 17:49:38 2015 (UTC)

Services\Tcpip key LastWrite time Sun Mar 20 17:13:59 2016 (UTC)

DhcpDomain =  
 DhcpIPAddress = 192.168.1.61  
 DhcpSubnetMask = 255.255.255.0  
 DhcpNameServer = 192.168.1.1  
 DhcpServer = 192.168.1.1

Interface {8B32CCEF-F092-453D-A04B-084246668014}

Name: Wireless Network Connection

Control\Network key LastWrite time Fri Feb 20 16:54:57 2015 (UTC)

Services\Tcpip key LastWrite time Fri Feb 20 16:53:49 2015 (UTC)

DhcpDomain =  
 DhcpIPAddress = 0.0.0.0  
 DhcpSubnetMask = 255.0.0.0  
 DhcpNameServer =  
 DhcpServer = 255.255.255.255

-----  
 nic2 v.20100401

(System) Gets NIC info from System hive

Adapter: {1BDD94C3-9D85-46F0-87E3-BD3288A5F6BD}

LastWrite Time: Sun Mar 13 00:22:58 2016 Z

UseZeroBroadcast	0
EnableDeadGWDetect	1
EnableDHCP	1
NameServer	
Domain	
RegistrationEnabled	1
RegisterAdapterName	0
DhcpIPAddress	172.20.10.5
DhcpSubnetMask	255.255.255.240
DhcpServer	172.20.10.1
Lease	85536
LeaseObtainedTime	Sun Mar 13 00:22:55 2016 Z
T1	Sun Mar 13 12:15:43 2016 Z
T2	Sun Mar 13 21:10:19 2016 Z
LeaseTerminatesTime	Mon Mar 14 00:08:31 2016 Z
AddressType	0
IsServerNapAware	0
DhcpConnForceBroadcastFlag	0
DhcpNameServer	172.20.10.1
DhcpDefaultGateway	172.20.10.1
DhcpSubnetMaskOpt	255.255.255.240
DhcpInterfaceOptions	- J y æV-¶
L J	y æV-¶

## SYSTEM OUTPUT

```
5 DhcpGatewayHardwareAddress      1
-   z_x_A^1d
DhcpGatewayHardwareCount          1
```

Adapter: {3ED9F155-8201-430C-85E1-EDD7020DE0CF}

LastWrite Time: Fri Feb 20 16:54:14 2015 Z

UseZeroBroadcast	0
EnableDeadGWDetect	1
EnableDHCP	1
NameServer	
Domain	
RegistrationEnabled	1
RegisterAdapterName	0
DhcpIPAddress	0.0.0.0
DhcpSubnetMask	255.0.0.0
DhcpServer	255.255.255.255
Lease	0
LeaseObtainedTime	Thu Jan 1 00:00:00 1970 Z
T1	Thu Jan 1 00:00:00 1970 Z
T2	Thu Jan 1 00:00:00 1970 Z
LeaseTerminatesTime	Thu Jan 1 00:00:00 1970 Z
AddressType	0
IsServerNapAware	0
DhcpConnForceBroadcastFlag	0

Adapter: {720B974A-3E6B-42BF-9839-4EE6CD676477}

LastWrite Time: Sun Mar 20 17:13:59 2016 Z

UseZeroBroadcast	0
EnableDeadGWDetect	1
EnableDHCP	1
NameServer	
Domain	
RegistrationEnabled	1
RegisterAdapterName	0
DhcpIPAddress	192.168.1.61
DhcpSubnetMask	255.255.255.0
DhcpServer	192.168.1.1
Lease	86400
LeaseObtainedTime	Sun Mar 20 17:13:59 2016 Z
T1	Mon Mar 21 05:13:59 2016 Z
T2	Mon Mar 21 14:13:59 2016 Z
LeaseTerminatesTime	Mon Mar 21 17:13:59 2016 Z
AddressType	0
IsServerNapAware	0
DhcpConnForceBroadcastFlag	0
DhcpNetworkHint	2427164646F636B6

## SYSTEM OUTPUT

```

MTU                                0
InterfaceMetric                    100
DhcpInterfaceOptions               L      J      x+ðVÀ"      Q      ◀
x+ðV LÿÿAbe-ArjunMalik -      J      x+ðVÀ"      J      x+ðVÀ" ÿ      J
      x+ðVÿÿÿ ;      J      x+ðV 'P:      J      x+ðV "À3      J      x+ðV
Q6      J      x+ðVÀ"      5      x+ðV|      ü      B←iV
DhcpGatewayHardware               À"      -      à?I{@
DhcpGatewayHardwareCount          1
DhcpDefaultGateway                192.168.1.1
DhcpNameServer                    192.168.1.1
DhcpSubnetMaskOpt                 255.255.255.0

```

Adapter: {749B2830-EBF4-4268-8BFD-189D3224ACFB}

LastWrite Time: Wed Apr 20 09:07:03 2016 Z

```

UseZeroBroadcast                   0
EnableDeadGWDetect                1
EnableDHCP                        1
NameServer
Domain
RegistrationEnabled                1
RegisterAdapterName               0
DhcpIPAddress                     192.168.1.179
DhcpSubnetMask                    255.255.255.0
DhcpServer                        192.168.1.1
Lease                              86400
LeaseObtainedTime                 Wed Apr 20 09:07:03 2016 Z
T1                                Wed Apr 20 21:07:03 2016 Z
T2                                Thu Apr 21 06:07:03 2016 Z
LeaseTerminatesTime               Thu Apr 21 09:07:03 2016 Z
AddressType                       0
IsServerNapAware                  0
DhcpConnForceBroadcastFlag        0
MTU                                0
InterfaceMetric                    100
DhcpInterfaceOptions               L      J      7~↑WÀ"      Q      ◀
7~↑W LÿÿAbe-ArjunMalik -      J      7~↑WÀ"      J      7~↑WÀ" ÿ      J
      7~↑Wÿÿÿ ;      J      7~↑W 'P:      J      7~↑W "À3      J      7~↑W Q6
      J      7~↑WÀ"      5      7~↑W|      ü      N;↑W
DhcpGatewayHardware               À"      -      à?I{@
DhcpGatewayHardwareCount          1
DhcpDefaultGateway                192.168.1.1
DhcpNameServer                    192.168.1.1
DhcpSubnetMaskOpt                 255.255.255.0

```

Adapter: {846ee342-7039-11de-9d20-806e6f6e6963}

LastWrite Time: Thu Feb 18 16:19:53 2016 Z

## SYSTEM OUTPUT

Adapter: {8B32CCEF-F092-453D-A04B-084246668014}

LastWrite Time: Fri Feb 20 16:53:49 2015 Z

UseZeroBroadcast	0
EnableDeadGWDetect	1
EnableDHCP	1
NameServer	
Domain	
RegistrationEnabled	1
RegisterAdapterName	0
DhcpIPAddress	0.0.0.0
DhcpSubnetMask	255.0.0.0
DhcpServer	255.255.255.255
Lease	0
LeaseObtainedTime	Thu Jan 1 00:00:00 1970 Z
T1	Thu Jan 1 00:00:00 1970 Z
T2	Thu Jan 1 00:00:00 1970 Z
LeaseTerminatesTime	Thu Jan 1 00:00:00 1970 Z
AddressType	0
IsServerNapAware	0
DhcpConnForceBroadcastFlag	0

Adapter: {A9E50A43-973B-4CAD-B78E-EA0321A4A293}

LastWrite Time: Wed Nov 11 20:31:51 2015 Z

UseZeroBroadcast	0
EnableDeadGWDetect	1
EnableDHCP	1
NameServer	
Domain	
RegistrationEnabled	1
RegisterAdapterName	0
DhcpIPAddress	0.0.0.0
DhcpSubnetMask	255.0.0.0
DhcpServer	255.255.255.255
Lease	0
LeaseObtainedTime	Thu Jan 1 00:00:00 1970 Z
T1	Thu Jan 1 00:00:00 1970 Z
T2	Thu Jan 1 00:00:00 1970 Z
LeaseTerminatesTime	Thu Jan 1 00:00:00 1970 Z
AddressType	0
IsServerNapAware	0
DhcpConnForceBroadcastFlag	0

Adapter: {FD2B5103-617C-4AE6-8DC4-A4772C463DDC}

LastWrite Time: Fri Feb 20 18:22:36 2015 Z

UseZeroBroadcast	0
EnableDeadGWDetect	1
EnableDHCP	1

## SYSTEM OUTPUT

```

NameServer
Domain
RegistrationEnabled      1
RegisterAdapterName      0
DhcpIPAddress            0.0.0.0
DhcpSubnetMask           255.0.0.0
DhcpServer               255.255.255.255
Lease                    0
LeaseObtainedTime        Thu Jan  1 00:00:00 1970 Z
T1                       Thu Jan  1 00:00:00 1970 Z
T2                       Thu Jan  1 00:00:00 1970 Z
LeaseTerminatesTime      Thu Jan  1 00:00:00 1970 Z
AddressType              0
IsServerNapAware         0
DhcpConnForceBroadcastFlag 0

```

```

-----
nolmhash v.20100712
(System) Gets NoLMHash value

```

```

nolmhash v.20100712
ControlSet001\Control\Lsa
LastWrite: Wed Apr 20 02:36:50 2016

```

NoLMHash value = 1

A value of 1 indicates that LMHashes are not stored in the SAM.

```

-----
pagefile v.20140505
(System) Get info on pagefile(s)

```

```

PagingFiles = ?:\pagefile.sys
ClearPageFileAtShutdown = 0
PagingFiles = ?:\pagefile.sys

```

```

-----
prefetch v.20120914
(SYSTEM) Gets the the Prefetch Parameters

```

EnablePrefetcher = 3

```

0 = Prefetching is disabled
1 = Application prefetching is enabled
2 = Boot prefetching is enabled
3 = Both boot and application prefetching is enabled

```

```

-----
productpolicy v.20091116
(System) Parse ProductPolicy value (Vista & Win2008 ONLY)

```

## SYSTEM OUTPUT

Note: This plugin applies to Vista and Windows 2008 ONLY.

For a listing of names and values, see:

<http://www.geoffchappell.com/viewer.htm?doc=notes/windows/license/install.htm&tx=3,5,6;4>

```

ACLUIFileFolderTool-IsSecurityUIEnabled - 1
ChangeDesktopBackground-Enabled - 1
DNS-Client-license-DAPolicy - 0
GroupPolicy-License-DomainIncapableSystem - 0
GroupPolicy-License-NetworkWaitTimeoutInSeconds - 30
GroupPolicy-License-WaitForNetwork - 0
IASLicensing-allowSubnetSyntax - 0
IASLicensing-maxClient - 0
IASLicensing-maxServerGroups - 0
Kernel-DynamicPartitioningSupported - 0
Kernel-ExpirationDate - 00000000000000000000000000000000
Kernel-MUI-Language-Allowed - EMPTY
Kernel-MUI-Language-Disallowed - EMPTY
Kernel-MUI-Language-SKU -
en-US;ar-SA;pt-BR;zh-TW;zh-CN;zh-HK;cs-CZ;da-DK;el-GR;es-ES;fi-FI;fr-FR;de-DE;he-IL;
hu-HU;it-IT;ja-JP;ko-KR;nl-NL;nb-NO;pl-PL;pt-PT;ru-RU;sv-SE;tr-TR;bg-BG;hr-HR;et-EE;
lv-LV;lt-LT;ro-RO;sr-Latn-CS;sk-SK;sl-SI;th-TH;uk-UA;fy-NL;qps-ploc;qps-plocm
Kernel-MUI-Number-Allowed - 1
Kernel-MaxPhysicalPage - 4096
Kernel-MemoryMirroringSupported - 0
Kernel-NativeVHDBoot - 0
Kernel-PersistDefectiveMemoryList - 0
Kernel-PhysicalMemoryAddAllowed - 0
Kernel-ProductInfo - 48
Kernel-RegisteredProcessors - 2
Kernel-VirtualDynamicPartitioningSupported - 0
Kernel-VmPhysicalMemoryAddAllowed - 0
Kernel-WindowsMaxMemAllowedia64 - 196608
Kernel-WindowsMaxMemAllowedx64 - 196608
Kernel-WindowsMaxMemAllowedx86 - 4096
LSA-Credman-DisableDomainCreds - 0
LSA-Policy-EnableTrustedDomains - 0
MCLicense-6F20786B-7DFC-4d72-B98B-FAA8699E5758-AdvancedConfigurationEnabled - 0
MCLicense-7CBE1823-362F-43b1-9AB6-92F18C216806-SupportedTunerCount - 0
MCLicense-9871786D-C2DE-4474-BDBB-C21A8B81B6C3-DVDRemotingEnabled - 0
MCLicense-CCE46F5E-2F26-49fd-82F8-00A2CB7C3E74-AEPEnabled - 0
MathRecognizerEventsLicensing-EnableMathRecognizer - 1
MediaCenter-EnabledSku - 1
Microsoft-Windows-AuxiliaryDisplay-EnableAPI - 1
Microsoft-Windows-AuxiliaryDisplay-EnableCPL - 1
Microsoft-Windows-AuxiliaryDisplay-EnableDriver - 1
Microsoft-Windows-AuxiliaryDisplay-EnableSDP - 1

```

## SYSTEM OUTPUT

Microsoft-Windows-Core-AllowMultiMon - 1  
 Microsoft-Windows-Core-AllowedControlledDevicesForBoot - 12  
 Microsoft-Windows-Core-InstanceLimitExemptedApps -  
 Microsoft-Windows-Core-MaxConcurrentIApp - 0  
 Microsoft-Windows-Core-MaxHRes - 4294967295  
 Microsoft-Windows-Core-MaxTopLevelWinPerApp - 0  
 Microsoft-Windows-Core-MaxVRes - 4294967295  
 Microsoft-Windows-Core-NeedsFullOEMVerification - 1  
 Microsoft-Windows-Core-ParentProcessDenylist -  
 Microsoft-Windows-DOT11PREF-AllowAdhoc - 1  
 Microsoft-Windows-DesktopWindowManager-Core-AnimatedTransitionsAllowed - 1  
 Microsoft-Windows-DesktopWindowManager-Core-CompositionAllowed - 1  
 Microsoft-Windows-DesktopWindowManager-Core-Flip3dAllowed - 1  
 Microsoft-Windows-DesktopWindowManager-Core-LivePreviewAllowed - 1  
 Microsoft-Windows-DesktopWindowManager-Core-ThumbnailsAllowed - 1  
 Microsoft-Windows-DesktopWindowManager-Core-TransparencyAllowed - 1  
 Microsoft-Windows-Fax-Common-DeviceLimit - 1  
 Microsoft-Windows-Fax-Common-EnableServerPolicy - 0  
 Microsoft-Windows-HotStart-EnableHotStart - 1  
 Microsoft-Windows-IE-InternetExplorer-SupportEnableAutoUpgrade - 1  
 Microsoft-Windows-InternetConnectionSharingConfig-HomeNetBeacon - 1  
 Microsoft-Windows-InternetConnectionSharingConfig-HomeNetICS - 1  
 Microsoft-Windows-NetworkBridge-WindowsHomeNwkEnabled - 1  
 Microsoft-Windows-OfflineFiles-Core-BranchCachingEnabled - 0  
 Microsoft-Windows-OfflineFiles-Core-FeatureEnabled - 1  
 Microsoft-Windows-QWAVE-EnableAdaptiveFlow - 1  
 Microsoft-Windows-QWAVE-Layer3Probing - 1  
 Microsoft-Windows-SensorsLicense-EnableCPL - 1  
 MicrosoftWindowsSafeDocsMain-BackupToNetShare - 1  
 MicrosoftWindowsSafeDocsMain-GPSupport - 1  
 MicrosoftWindowsSafeDocsMain-PerUserBackup - 1  
 MobilePCMobilityCenter-EnableMobilityCenter - 1  
 MobilePCPresentationSettings-EnablePresentationSettings - 1  
 NetworkProjection-CanRunNetworkProjection - 1  
 NetworkProjection-CanStartPresenting - 1  
 NetworkSecurity-IPsecDoSProtection-EnabledPolicy - 0  
 OMD-API-Enabled - 1  
 PeerDist-Common-Client-Enabled - 1  
 PeerDist-Common-HostedCache-Enabled - 0  
 PeerDist-Common-KMDriver-Enabled - 0  
 PeerDist-Common-Server-Enabled - 0  
 PeerToPeerBase-Collaboration-EnabledPolicy - 1  
 PeerToPeerBase-Graphing-EnabledPolicy - 1  
 PeerToPeerBase-Grouping-EnabledPolicy - 1  
 PeerToPeerBase-IdManager-EnabledPolicy - 1  
 PeerToPeerBase-Pnrp-EnabledPolicy - 1  
 Personalization-Enabled - 1  
 PhotoMinFeature-AdvancedSlideshow - 0

## SYSTEM OUTPUT

PhotoMinFeature-MakeDVD - 0  
 Printing-Spooler-Core-Localspl-Licensing-Enabled - 1  
 Printing-Spooler-Core-Spoolss-Licensing-Enabled - 1  
 Printing-Spooler-Core-Spoolss-Licensing-Network-Default-Printer-Enabled - 1  
 Printing-Spooler-Pmc-Licensing-Enabled - 1  
 RasBase-DefaultConnections - 2  
 RasBase-MaxConnections - 3  
 SLC-Component-SKU-OCUR-OCURControlContentAllowed - 0  
 SMBServer-AllowHashPublication - 0  
 SMBServer-AllowRemoteLegacyShadowCopyAccess - 1  
 SMBServer-AllowRemoteShadowCopyAccess - 1  
 SMBServer-WindowsMaxInSMBConns - 20  
 SecureStartupFeature-Enabled - 1  
 SecureStartupFeature-Enabled-Driver - 1  
 SecureStartupFeature-Enabled-Premium - 0  
 SecureStartupFeature-PerfWarning - 0  
 Security-SPP-ActivationResetCount - 5  
 Security-SPP-ActivationResetCountMax - 2147483647  
 Security-SPP-ApplicationActivationResetCount - 5  
 Security-SPP-ApplicationActivationResetCountMax - 2147483647  
 Security-SPP-CMIDExpirationPeriod - 43200  
 Security-SPP-EvaluationModeEnabled - 0  
 Security-SPP-GenuineLocalStatus - 1  
 Security-SPP-KmsCountedIdList -  
 Security-SPP-Reserved-EnableNotificationMode - 1  
 Security-SPP-Reserved-SkuPpdConsumed - 1  
 Security-SPP-Reserved-TBLProductKeyType - 0  
 Security-SPP-Reserved-TBLRemainingTime - 0  
 Security-SPP-Reserved-TBLState - 0  
 Security-SPP-TokenActivation-AdditionalInfo -  
 Security-SPP-UX-Slui-SelectivelySetBlackBackground - 1  
 SnippingToolLicensing-Enabled - 1  
 StickyNotesLicensing-Enabled - 1  
 TabletPC-MathInputLicensing-EnableMathInput - 1  
 TabletPC-UIHub-EnableCursors - 1  
 TabletPC-UIHub-EnableFeedback - 1  
 TabletPC-UIHub-EnableFlicks - 1  
 TabletPC-tabbtn-EnableButtons - 1  
 TabletPCAccessories-EnableJournal - 1  
 TabletPCAccessories-EnableStickyNotes - 1  
 TabletPCCoreInkRecognitionLicensing-EnableText - 1  
 TabletPCInputPanel-EnableTIP - 1  
 TabletPCInputPanel-EnableTIPSynced - 1  
 TabletPCInputPersonalization-EnablePersonalization - 1  
 TabletPCPlatformInput-core-EnableTouchUI - 1  
 TabletPCPlatformInput-core-MultiTouchGestures - 1  
 TabletPCPlatformInput-core-SFP - 1  
 TerminalServices-DeviceRedirection-Licenses-PnpRedirectionAllowed - 0



## SYSTEM OUTPUT

TerminalServices-DeviceRedirection-Licenses-TSAudioCaptureAllowed - 0  
 TerminalServices-DeviceRedirection-Licenses-TSEasyPrintAllowed - 0  
 TerminalServices-DeviceRedirection-Licenses-TSMFPluginAllowed - 0  
 TerminalServices-RDP-7-Advanced-Compression-Allowed - 0  
 TerminalServices-RemoteConnectionManager-0f0a4bf8-8362-435d-938c-222a518a8b78-Disabled - 0  
 TerminalServices-RemoteConnectionManager-45344fe7-00e6-4ac6-9f01-d01fd4ffadfb-LocalOnly - 0  
 TerminalServices-RemoteConnectionManager-45344fe7-00e6-4ac6-9f01-d01fd4ffadfb-MaxSessions - 1  
 TerminalServices-RemoteConnectionManager-8dc86f1d-9969-4379-91c1-06fe1dc60575-InitialProgram - %SystemRoot%\ehome\mcrmgr.exe  
 TerminalServices-RemoteConnectionManager-8dc86f1d-9969-4379-91c1-06fe1dc60575-MaxSessions - 5  
 TerminalServices-RemoteConnectionManager-AllowAppServerMode - 0  
 TerminalServices-RemoteConnectionManager-AllowD3DRemoting - 0  
 TerminalServices-RemoteConnectionManager-AllowMultimon - 0  
 TerminalServices-RemoteConnectionManager-AllowMultipleSessions - 1  
 TerminalServices-RemoteConnectionManager-AllowRemoteConnections - 1  
 TerminalServices-RemoteConnectionManager-MaxUserSessions - 0  
 TerminalServices-RemoteConnectionManager-UiEffects-DWMRemotingAllowed - 0  
 TerminalServices-RemoteConnectionManager-b7857721-7a62-4a37-aff3-253fe2b8b0e8-MaxSessions - 0  
 VirtualPC-licensing-Enabled - 1  
 VirtualXP-licensing-Enabled - 1  
 WMPPlayer-HMEAllowed - 1  
 WMPPlayer-RMEAllowed - 1  
 WMPPlayer-RMESecurityGroupAllowed - 0  
 WindowsAnytimeUpgrade-CanUpgrade - 1  
 WindowsSearchComponent-ComponentInstalled - 1  
 WorkstationService-DomainJoinEnabled - 1  
 appid-EnableV2 - 0  
 explorer-AeroAnimationAllowed - 1  
 explorer-AeroShakeAllowed - 1  
 feclient-EfsEnabled - 1  
 feclient-EfsUserCacheLimit - 5  
 msac3enc-DolbyDigitalEncoderV2AddIn - 0  
 msac3enc-DolbyDigitalEncoderV2AddInEnable - 1  
 msac3enc-DolbyDigitalEncoderV2InSKU - 1  
 msmpeg2adec-AACDecoderV2AddIn - 0  
 msmpeg2adec-AACDecoderV2AddInEnable - 1  
 msmpeg2adec-AACDecoderV2InSKU - 1  
 msmpeg2adec-DolbyDigitalDecoderV2AddIn - 0  
 msmpeg2adec-DolbyDigitalDecoderV2AddInEnable - 1  
 msmpeg2adec-DolbyDigitalDecoderV2InSKU - 1  
 msmpeg2enc-MPEG2VideoEncoderV2AddIn - 0  
 msmpeg2enc-MPEG2VideoEncoderV2AddInEnable - 1  
 msmpeg2enc-MPEG2VideoEncoderV2InSKU - 1

## SYSTEM OUTPUT

```

msmpeg2vdec-H264VideoDecoderV2AddIn - 0
msmpeg2vdec-H264VideoDecoderV2AddInEnable - 1
msmpeg2vdec-H264VideoDecoderV2InSKU - 1
msmpeg2vdec-MPEG2VideoDecoderV2AddIn - 0
msmpeg2vdec-MPEG2VideoDecoderV2AddInEnable - 1
msmpeg2vdec-MPEG2VideoDecoderV2InSKU - 1
parentalcontrols-EnableFeature - 1
provsvc-license-HomeGroupCreate - 1
shell-homegroup-Enabled - 1
shell32-license-GroupPolicy-TryHarderPinned - 0
volmgrx-SupportDynamic - 1
volmgrx-SupportMirror - 1
volmgrx-SupportRaid5 - 0

```

```

-----
producttype v.20100325
(System) Queries System hive for Windows Product info

```

```

ControlSet001\Control\ProductOptions
LastWrite = Thu Sep 10 16:09:06 2015

```

```

Ref: http://support.microsoft.com/kb/152078
    http://support.microsoft.com/kb/181412

```

```

ProductType = WinNT
Ref: http://technet.microsoft.com/en-us/library/cc782360%28WS.10%29.aspx
WinNT indicates a workstation.
ServerNT indicates a standalone server.
LanmanNT indicates a domain controller (pri/backup).

```

```

ProductSuite = Terminal Server
Ref: http://technet.microsoft.com/en-us/library/cc784364%28WS.10%29.aspx

```

```

-----
rdpport v.20100713
(System) Queries System hive for RDP Port

```

```
rdpport v.20100713
```

```
Remote Desktop Listening Port Number = 3389
```

```

-----
routes v.20100817
(System) Get persistent routes

```

```

ControlSet001\Services\Tcpip\Parameters\PersistentRoutes
LastWrite: Sun Nov 21 03:39:53 2010

```

```
ControlSet001\Services\Tcpip\Parameters\PersistentRoutes has no values.
```

```

-----
safeboot v.20081216

```

## SYSTEM OUTPUT

(System) Check SafeBoot entries

Minimal [Thu Sep 10 17:10:00 2015 Z]

Tue Jul 14 04:49:01 2009 Z

Power (Service)

ProfSvc (Service)

WinDefend (Service)

Tue Jul 14 04:53:35 2009 Z

AppInfo (Service)

AppMgmt (Service)

Base (Driver Group)

Boot Bus Extender (Driver Group)

Boot file system (Driver Group)

CryptSvc (Service)

DcomLaunch (Service)

EFS (Service)

EventLog (Service)

File system (Driver Group)

Filter (Driver Group)

HelpSvc (Service)

KeyIso (Service)

Netlogon (Service)

NTDS (Service)

PCI Configuration (Driver Group)

PlugPlay (Service)

PNP Filter (Driver Group)

Primary disk (Driver Group)

RpcEptMapper (Service)

RpcSs (Service)

sacsvr (Service)

SCSI Class (Driver Group)

sermouse.sys (Driver)

SWPRV (Service)

System Bus Extender (Driver Group)

TabletInputService (Service)

TBS (Service)

TrustedInstaller (Service)

VDS (Service)

vga.sys (Driver)

vgasave.sys (Driver)

vmms (Service)

volmgr.sys (Driver)

volmgrx.sys (Driver)

WinMgmt (Service)

{36FC9E60-C465-11CF-8056-444553540000} (Universal Serial Bus controllers)

{4D36E965-E325-11CE-BFC1-08002BE10318} (CD-ROM Drive)

{4D36E967-E325-11CE-BFC1-08002BE10318} (DiskDrive)

{4D36E969-E325-11CE-BFC1-08002BE10318} (Standard floppy disk controller)

## SYSTEM OUTPUT

{4D36E96A-E325-11CE-BFC1-08002BE10318} (Hdc)  
 {4D36E96B-E325-11CE-BFC1-08002BE10318} (Keyboard)  
 {4D36E96F-E325-11CE-BFC1-08002BE10318} (Mouse)  
 {4D36E977-E325-11CE-BFC1-08002BE10318} (PCMCIA Adapters)  
 {4D36E97B-E325-11CE-BFC1-08002BE10318} (SCSIAdapter)  
 {4D36E97D-E325-11CE-BFC1-08002BE10318} (System)  
 {4D36E980-E325-11CE-BFC1-08002BE10318} (Floppy disk drive)  
 {533C5B84-EC70-11D2-9505-00C04F79DEAF} (Volume shadow copy)  
 {6BDD1FC1-810F-11D0-BEC7-08002BE2092F} (IEEE 1394 Bus host controllers)  
 {71A27CDD-812A-11D0-BEC7-08002BE2092F} (Volume)  
 {745A17A0-74D3-11D0-B6FE-00A0C90F57DA} (Human Interface Devices)  
 {D48179BE-EC20-11D1-B6B8-00C04FA372A7} (SBP2 IEEE 1394 Devices)  
 {D94EE5D8-D189-4994-83D2-F68D7D41B0E6} (SecurityDevices)

Tue Jul 14 04:54:07 2009 Z

WudfPf (Driver)  
 WudfRd (Driver)  
 WudfSvc (Service)

Thu Sep 10 17:09:09 2015 Z

mcpltsvc ()

Thu Sep 10 17:13:12 2015 Z

MCODS ()

Network [Fri Feb 19 09:20:24 2016 Z]

Tue Jul 14 04:49:01 2009 Z

MPSPdrv (Driver)  
 MPSSvc (Service)  
 Power (Service)  
 ProfSvc (Service)  
 WinDefend (Service)

Tue Jul 14 04:49:20 2009 Z

NlaSvc (Service)

Tue Jul 14 04:53:35 2009 Z

AFD (Service)  
 AppInfo (Service)  
 AppMgmt (Service)  
 Base (Driver Group)  
 BFE (Service)  
 Boot Bus Extender (Driver Group)  
 Boot file system (Driver Group)  
 bowser (Driver)  
 Browser (Service)  
 CryptSvc (Service)  
 DcomLaunch (Service)  
 dfsc (Driver)  
 Dhcp (Service)  
 DnsCache (Service)  
 Dot3Svc (Service)  
 Eaphost (Service)

## SYSTEM OUTPUT

EFS (Service)  
EventLog (Service)  
File system (Driver Group)  
Filter (Driver Group)  
HelpSvc (Service)  
IKEEXT (Service)  
ipnat.sys (Driver)  
KeyIso (Service)  
LanmanServer (Service)  
LanmanWorkstation (Service)  
LmHosts (Service)  
Messenger (Service)  
mrxsmmb (Driver)  
mrxsmmb10 (Driver)  
mrxsmmb20 (Driver)  
NativeWifiP (Service)  
NDIS (Driver Group)  
NDIS Wrapper (Driver Group)  
Ndisuio (Service)  
NetBIOS (Service)  
NetBIOSGroup (Driver Group)  
NetBT (Service)  
NetDDEGroup (Driver Group)  
Netlogon (Service)  
NetMan (Service)  
netprofm (Service)  
Network (Driver Group)  
NetworkProvider (Driver Group)  
Nsi (Service)  
nsiproxy.sys (Driver)  
NTDS (Service)  
PCI Configuration (Driver Group)  
PlugPlay (Service)  
PNP Filter (Driver Group)  
PNP\_TDI (Driver Group)  
PolicyAgent (Service)  
Primary disk (Driver Group)  
rdbss (Driver)  
rdpencldd.sys (Driver)  
rdsessmgr (Service)  
RpcEptMapper (Service)  
RpcSs (Service)  
sacsvr (Service)  
SCardSvr (Service)  
SCSI Class (Driver Group)  
sermouse.sys (Driver)  
SharedAccess (Service)  
Streams Drivers (Driver Group)

## SYSTEM OUTPUT

SWPRV (Service)  
 System Bus Extender (Driver Group)  
 TabletInputService (Service)  
 TBS (Service)  
 Tcpip (Service)  
 TDI (Driver Group)  
 TrustedInstaller (Service)  
 VDS (Service)  
 vga.sys (Driver)  
 vgasave.sys (Driver)  
 vmms (Service)  
 volmgr.sys (Driver)  
 volmgrx.sys (Driver)  
 WinMgmt (Service)  
 Wlansvc (Service)  
 WudfUsbccidDriver (Driver)  
 {36FC9E60-C465-11CF-8056-444553540000} (Universal Serial Bus controllers)  
 {4D36E965-E325-11CE-BFC1-08002BE10318} (CD-ROM Drive)  
 {4D36E967-E325-11CE-BFC1-08002BE10318} (DiskDrive)  
 {4D36E969-E325-11CE-BFC1-08002BE10318} (Standard floppy disk controller)  
 {4D36E96A-E325-11CE-BFC1-08002BE10318} (Hdc)  
 {4D36E96B-E325-11CE-BFC1-08002BE10318} (Keyboard)  
 {4D36E96F-E325-11CE-BFC1-08002BE10318} (Mouse)  
 {4D36E972-E325-11CE-BFC1-08002BE10318} (Net)  
 {4D36E973-E325-11CE-BFC1-08002BE10318} (NetClient)  
 {4D36E974-E325-11CE-BFC1-08002BE10318} (NetService)  
 {4D36E975-E325-11CE-BFC1-08002BE10318} (NetTrans)  
 {4D36E977-E325-11CE-BFC1-08002BE10318} (PCMCIA Adapters)  
 {4D36E97B-E325-11CE-BFC1-08002BE10318} (SCSIAdapter)  
 {4D36E97D-E325-11CE-BFC1-08002BE10318} (System)  
 {4D36E980-E325-11CE-BFC1-08002BE10318} (Floppy disk drive)  
 {50DD5230-BA8A-11D1-BF5D-0000F805F530} (Smart card readers)  
 {533C5B84-EC70-11D2-9505-00C04F79DEAF} (Volume shadow copy)  
 {6BDD1FC1-810F-11D0-BEC7-08002BE2092F} (IEEE 1394 Bus host controllers)  
 {71A27CDD-812A-11D0-BEC7-08002BE2092F} (Volume)  
 {745A17A0-74D3-11D0-B6FE-00A0C90F57DA} (Human Interface Devices)  
 {D48179BE-EC20-11D1-B6B8-00C04FA372A7} (SBP2 IEEE 1394 Devices)  
 {D94EE5D8-D189-4994-83D2-F68D7D41B0E6} (SecurityDevices)  
 Tue Jul 14 04:53:49 2009 Z  
 VaultSvc (Service)  
 Tue Jul 14 04:54:07 2009 Z  
 WudfPf (Driver)  
 WudfRd (Driver)  
 WudfSvc (Service)  
 Tue Jul 14 04:54:37 2009 Z  
 ndiscap (Driver)  
 Thu Sep 10 17:06:31 2015 Z  
 mfemms (Service)

## SYSTEM OUTPUT

```

Thu Sep 10 17:06:43 2015 Z
  mfehdk (Service)
  mfehdk.sys (Driver)
  mfetdi2k (Service)
  mfetdi2k.sys (Driver)
  mfevtp (Service)
Thu Sep 10 17:06:52 2015 Z
  mfeaack (Service)
  mfeaack.sys (Driver)
Thu Sep 10 17:06:57 2015 Z
  mfeavfk (Service)
  mfeavfk.sys (Driver)
Thu Sep 10 17:08:44 2015 Z
  mfefirek (Service)
  mfefirek.sys (Driver)
Thu Sep 10 17:08:52 2015 Z
  mfefire (Service)
Thu Sep 10 17:09:09 2015 Z
  mcpltsvc ()
Thu Sep 10 17:09:33 2015 Z
  McMPFSvc (Service)
Thu Sep 10 17:12:57 2015 Z
  mfencbdc
  mfencbdc.sys
Thu Sep 10 17:13:12 2015 Z
  McNaiAnn ()
  MCODS ()
Fri Feb 19 09:20:24 2016 Z
  mcapexe ()

```

-----  
 services v.20080507

(System) Lists services/drivers in Services key by LastWrite times

ControlSet001\Services

Lists services/drivers in Services key by LastWrite times

Wed Apr 20 02:39:31 2016Z

```

Name      = AsyncMac
Display   = @%systemroot%\system32\rascfg.dll,-32000
ImagePath = system32\DRIVERS\asyncmac.sys
Type      = Kernel driver
Start     = Manual
Group     =

```

Wed Apr 20 02:39:13 2016Z

```

Name      = mfeaack
Display   = McAfee Inc. mfeaack

```

## SYSTEM OUTPUT

ImagePath = system32\drivers\mfeaack.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = mfencbdc  
 Display = McAfee Inc. mfencbdc  
 ImagePath = system32\DRIVERS\mfencbdc.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Wed Apr 20 02:37:21 2016Z

Name = mfefirek  
 Display = McAfee Inc. mfefirek  
 ImagePath = system32\drivers\mfefirek.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Wed Apr 20 02:37:20 2016Z

Name = cfwids  
 Display = McAfee Inc. cfwids  
 ImagePath = system32\drivers\cfwids.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Wed Apr 20 02:37:01 2016Z

Name = mfemms  
 Display = McAfee Service Controller  
 ImagePath = "C:\Program Files\Common Files\McAfee\SystemCore\mfemms.exe"  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

Wed Apr 20 02:36:56 2016Z

Name = vwifimp  
 Display = Microsoft Virtual WiFi Miniport Service  
 ImagePath = system32\DRIVERS\vwifimp.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = NDIS

Wed Apr 20 02:36:49 2016Z

Name = BrSerIb  
 Display = Brother Serial Interface Driver(WDM)  
 ImagePath = system32\DRIVERS\BrSerIb.sys



## SYSTEM OUTPUT

Type = Kernel driver  
 Start = Manual  
 Group =

Name = BrUsbSib  
 Display = Brother Serial USB Driver(WDM)  
 ImagePath = system32\DRIVERS\BrUsbSib.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = BthEnum  
 Display = Bluetooth Enumerator Service  
 ImagePath = system32\DRIVERS\BthEnum.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = BthPan  
 Display = Bluetooth Device (Personal Area Network)  
 ImagePath = system32\DRIVERS\bthpan.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = NDIS

Name = monitor  
 Display = Microsoft Monitor Class Function Driver Service  
 ImagePath = system32\DRIVERS\monitor.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = mouhid  
 Display = Mouse HID Driver  
 ImagePath = system32\DRIVERS\mouhid.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Pointer Port

Name = RFCOMM  
 Display = Bluetooth Device (RFCOMM Protocol TDI)  
 ImagePath = system32\DRIVERS\rfcomm.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = PNP\_TDI

Name = usbprint  
 Display = Microsoft USB PRINTER Class

## SYSTEM OUTPUT

ImagePath = system32\DRIVERS\usbprint.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = extended base

Name = usbscan  
 Display = USB Scanner Driver  
 ImagePath = system32\DRIVERS\usbscan.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Base

Wed Apr 20 02:36:48 2016Z

Name = BTHUSB  
 Display = Bluetooth Radio USB Driver  
 ImagePath = System32\Drivers\BTHUSB.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = PNP Filter

Name = HidUsb  
 Display = Microsoft HID Class Driver  
 ImagePath = system32\DRIVERS\hidusb.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = extended base

Name = kbdhid  
 Display = Keyboard HID Driver  
 ImagePath = system32\DRIVERS\kbdhid.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Keyboard Port

Name = scfilter  
 Display = @%SystemRoot%\System32\drivers\scfilter.sys, -11  
 ImagePath = System32\DRIVERS\scfilter.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = PnP Filter

Name = WinUSB  
 Display = WinUSB Service  
 ImagePath = system32\DRIVERS\WinUSB.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Base

## SYSTEM OUTPUT

Name = WUDFRd  
 Display =  
 ImagePath = system32\DRIVERS\WUDFRd.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Wed Apr 20 02:36:46 2016Z

Name = SPUVCbv  
 Display = SPUVCb Driver Service  
 ImagePath = System32\Drivers\SPUVCbv\_x64.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Wed Apr 20 02:36:44 2016Z

Name = usbccgp  
 Display = Microsoft USB Generic Parent Driver  
 ImagePath = system32\DRIVERS\usbccgp.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Base

Wed Apr 20 02:36:42 2016Z

Name = mfeavfk  
 Display = McAfee Inc. mfeavfk  
 ImagePath = system32\drivers\mfeavfk.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Wed Apr 20 02:36:41 2016Z

Name = AgereSoftModem  
 Display = Agere Systems Soft Modem  
 ImagePath = system32\DRIVERS\agrsm64.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = HdAudAddService  
 Display = Microsoft 1.1 UAA Function Driver for High Definition Audio Service  
 ImagePath = system32\drivers\HdAudio.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = IntcDAud  
 Display = Intel(R) Display Audio

## SYSTEM OUTPUT

ImagePath = system32\DRIVERS\IntcDAud.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = ksthunk  
 Display = Kernel Streaming Thunks  
 ImagePath = \SystemRoot\system32\drivers\ksthunk.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = PNP Filter

Name = Modem  
 Display =  
 ImagePath = system32\drivers\modem.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended base

Name = nusb3hub  
 Display = Renesas Electronics USB 3.0 Hub Driver  
 ImagePath = \SystemRoot\system32\drivers\nusb3hub.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Base

Name = Parport  
 Display = Parallel port driver  
 ImagePath = \SystemRoot\system32\drivers\parport.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Parallel arbitrator

Name = usbhub  
 Display = Microsoft USB Standard Hub Driver  
 ImagePath = system32\DRIVERS\usbhub.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Base

Wed Apr 20 02:36:38 2016Z

Name = mssmbios  
 Display = Microsoft System Management BIOS Driver  
 ImagePath = \SystemRoot\system32\drivers\mssmbios.sys  
 Type = Kernel driver  
 Start = System Start  
 Group =

## SYSTEM OUTPUT

Wed Apr 20 02:36:34 2016Z

Name = cdrom  
 Display = CD-ROM Driver  
 ImagePath = system32\DRIVERS\cdrom.sys  
 Type = Kernel driver  
 Start = System Start  
 Group = SCSI CDROM Class

Name = Disk  
 Display = Disk Driver  
 ImagePath = system32\drivers\disk.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group =

Name = hpdskflt  
 Display = HP Filter  
 ImagePath = system32\drivers\hpdskflt.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = PnP Filter

Name = rdyboost  
 Display = ReadyBoost  
 ImagePath = System32\drivers\rdyboost.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = PnP Filter

Wed Apr 20 02:36:33 2016Z

Name = 1394ohci  
 Display = 1394 OHCI Compliant Host Controller  
 ImagePath = \SystemRoot\system32\drivers\1394ohci.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = Accelerometer  
 Display = HP Mobile Data Protection Sensor  
 ImagePath = \SystemRoot\system32\drivers\Accelerometer.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Base

Name = ACPI  
 Display = Microsoft ACPI Driver  
 ImagePath = system32\drivers\ACPI.sys  
 Type = Kernel driver

## SYSTEM OUTPUT

```

Start      = Boot Start
Group      = Boot Bus Extender

Name       = AFD
Display    = @%systemroot%\system32\drivers\afd.sys, -1000
ImagePath  = \SystemRoot\system32\drivers\afd.sys
Type       = Kernel driver
Start      = System Start
Group      = PNP_TDI

Name       = amdkgdag
Display    =
ImagePath  = system32\DRIVERS\atikmdag.sys
Type       = Kernel driver
Start      = Manual
Group      = Video

Name       = amdkgpfd
Display    = AMD PCI Root Bus Lower Filter
ImagePath  = system32\drivers\amdkgpfd.sys
Type       = Kernel driver
Start      = Boot Start
Group      = PnP Filter

Name       = atapi
Display    = IDE Channel
ImagePath  = system32\drivers\atapi.sys
Type       = Kernel driver
Start      = Boot Start
Group      = SCSI Miniport

Name       = Beep
Display    = Beep
ImagePath  =
Type       = Kernel driver
Start      = System Start
Group      = Base

Name       = blbdrive
Display    =
ImagePath  = \SystemRoot\system32\drivers\blbdrive.sys
Type       = Kernel driver
Start      = System Start
Group      =

Name       = bowser
Display    = @%systemroot%\system32\browse.dll, -102
ImagePath  = system32\DRIVERS\browse.sys

```

## SYSTEM OUTPUT

Type = File system driver  
 Start = Manual  
 Group = Network

Name = cdfs  
 Display = CD/DVD File System Reader  
 ImagePath = system32\DRIVERS\cdfs.sys  
 Type = File system driver  
 Start = Disabled  
 Group = Boot File System

Name = CLFS  
 Display = @%SystemRoot%\system32\clfs.sys, -100  
 ImagePath = System32\CLFS.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = Filter

Name = CmBatt  
 Display = Microsoft ACPI Control Method Battery Driver  
 ImagePath = \SystemRoot\system32\drivers\CmBatt.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = CNG  
 Display =  
 ImagePath = System32\Drivers\cng.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = Base

Name = Compbatt  
 Display = Microsoft Composite Battery Driver  
 ImagePath = system32\drivers\compbatt.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = System Bus Extender

Name = CompositeBus  
 Display = Composite Bus Enumerator Driver  
 ImagePath = \SystemRoot\system32\drivers\CompositeBus.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Name = CSC  
 Display = @%systemroot%\system32\cscsvc.dll, -202

## SYSTEM OUTPUT

ImagePath = system32\drivers\csc.sys

Type = Kernel driver

Start = System Start

Group = network

Name = DfsC

Display = @%systemroot%\system32\drivers\dfsc.sys,-101

ImagePath = System32\Drivers\dfsc.sys

Type = File system driver

Start = System Start

Group = Network

Name = discache

Display = @%systemroot%\system32\drivers\discache.sys,-102

ImagePath = System32\drivers\discache.sys

Type = Kernel driver

Start = System Start

Group =

Name = DXGKrnl

Display = LDDM Graphics Subsystem

ImagePath = \SystemRoot\System32\drivers\dxgkrnl.sys

Type = Kernel driver

Start = Manual

Group = Video Init

Name = e1cexpress

Display = Intel(R) PRO/1000 PCI Express Network Connection Driver C

ImagePath = system32\DRIVERS\e1c62x64.sys

Type = Kernel driver

Start = Manual

Group = NDIS

Name = exfat

Display = exFAT File System Driver

ImagePath =

Type = File system driver

Start = Manual

Group = Boot File System

Name = fastfat

Display = FAT12/16/32 File System Driver

ImagePath =

Type = File system driver

Start = Manual

Group = Boot File System

Name = FileInfo



## SYSTEM OUTPUT

Display = @%SystemRoot%\system32\drivers\fileinfo.sys,-100  
 ImagePath = system32\drivers\fileinfo.sys  
 Type = File system driver  
 Start = Boot Start  
 Group = FSFilter Bottom

Name = FltMgr  
 Display = @%SystemRoot%\system32\drivers\fltMgr.sys,-10001  
 ImagePath = system32\drivers\fltMgr.sys  
 Type = File system driver  
 Start = Boot Start  
 Group = FSFilter Infrastructure

Name = Fs\_Rec  
 Display =  
 ImagePath =  
 Type = 0x0  
 Start = Boot Start  
 Group = File System

Name = fvevol  
 Display = @%SystemRoot%\system32\drivers\fvevol.sys,-100  
 ImagePath = System32\DRIVERS\fvevol.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = PnP Filter

Name = HDAudBus  
 Display = Microsoft UAA Bus Driver for High Definition Audio  
 ImagePath = \SystemRoot\system32\drivers\HDAudBus.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Name = HTTP  
 Display = @%SystemRoot%\system32\drivers\http.sys,-1  
 ImagePath = system32\drivers\HTTP.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = hwpolicy  
 Display = @%systemroot%\system32\drivers\hwpolicy.sys,-101  
 ImagePath = System32\drivers\hwpolicy.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group =

## SYSTEM OUTPUT

Name = i8042prt  
 Display = i8042 Keyboard and PS/2 Mouse Port Driver  
 ImagePath = \SystemRoot\system32\drivers\i8042prt.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Keyboard Port

Name = igfx  
 Display =  
 ImagePath = system32\DRIVERS\igdkmd64.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Video

Name = intelppm  
 Display = Intel Processor Driver  
 ImagePath = system32\DRIVERS\intelppm.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Name = JMCR  
 Display =  
 ImagePath = system32\DRIVERS\jmcr.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = kbdclass  
 Display = Keyboard Class Driver  
 ImagePath = system32\DRIVERS\kbdclass.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Keyboard Class

Name = KSecDD  
 Display =  
 ImagePath = System32\Drivers\ksecdd.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = Base

Name = KSecPkg  
 Display =  
 ImagePath = System32\Drivers\ksecpkg.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = Cryptography

## SYSTEM OUTPUT

Name = lltdio  
 Display = Link-Layer Topology Discovery Mapper I/O Driver  
 ImagePath = system32\DRIVERS\lltdio.sys  
 Type = Kernel driver  
 Start = Auto Start  
 Group = NDIS

Name = luafv  
 Display = @%systemroot%\system32\drivers\luafv.sys,-100  
 ImagePath = \SystemRoot\system32\drivers\luafv.sys  
 Type = File system driver  
 Start = Auto Start  
 Group = FSFilter Virtualization

Name = MBAMProtector  
 Display =  
 ImagePath = \??\C:\Windows\system32\drivers\mbam.sys  
 Type = File system driver  
 Start = Manual  
 Group = FSFilter Anti-Virus

Name = MBAMSwissArmy  
 Display = MBAMSwissArmy  
 ImagePath = \??\C:\Windows\system32\drivers\MBAMSwissArmy.sys  
 Type = File system driver  
 Start = Manual  
 Group = FSFilter Activity Monitor

Name = MBAMWebAccessControl  
 Display =  
 ImagePath = \??\C:\Windows\system32\drivers\mwac.sys  
 Type = File system driver  
 Start = Manual  
 Group =

Name = MEIx64  
 Display = Intel(R) Management Engine Interface  
 ImagePath = \SystemRoot\system32\drivers\HECIx64.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Name = mfehidk  
 Display = McAfee Inc. mfehidk  
 ImagePath = system32\drivers\mfehidk.sys  
 Type = Kernel driver  
 Start = Boot Start

## SYSTEM OUTPUT

Group = FSFilter Anti-Virus

Name = mfencrk  
 Display = McAfee Inc. mfencrk  
 ImagePath = system32\DRIVERS\mfencrk.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = mfesapns  
 Display = McAfee Process Start Notification Service  
 ImagePath = \??\C:\Program Files (x86)\McAfee\SiteAdvisor\x64\mfesapns.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = mfewfpk  
 Display = McAfee Inc. mfewfpk  
 ImagePath = system32\drivers\mfewfpk.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = PNP\_TDI

Name = mouclass  
 Display = Mouse Class Driver  
 ImagePath = system32\DRIVERS\mouclass.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Pointer Class

Name = mountmgr  
 Display = @%SystemRoot%\system32\drivers\mountmgr.sys, -100  
 ImagePath = System32\drivers\mountmgr.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = System Bus Extender

Name = mpsdrv  
 Display = @%SystemRoot%\system32\FirewallAPI.dll, -23092  
 ImagePath = System32\drivers\mpsdrv.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = network

Name = mrxsmbs  
 Display = @%systemroot%\system32\wkssvc.dll, -1002  
 ImagePath = system32\DRIVERS\mrxsmbs.sys  
 Type = File system driver

## SYSTEM OUTPUT

Start = Manual  
Group = Network

Name = mrxsmb10  
Display = @%systemroot%\system32\wkssvc.dll, -1004  
ImagePath = system32\DRIVERS\mrxsmb10.sys  
Type = File system driver  
Start = Manual  
Group = Network

Name = mrxsmb20  
Display = @%systemroot%\system32\wkssvc.dll, -1006  
ImagePath = system32\DRIVERS\mrxsmb20.sys  
Type = File system driver  
Start = Manual  
Group = Network

Name = msahci  
Display =  
ImagePath = system32\drivers\msahci.sys  
Type = Kernel driver  
Start = Boot Start  
Group = SCSI Miniport

Name = Msfs  
Display =  
ImagePath =  
Type = File system driver  
Start = System Start  
Group = File system

Name = msisadrv  
Display =  
ImagePath = system32\drivers\msisadrv.sys  
Type = Kernel driver  
Start = Boot Start  
Group = Boot Bus Extender

Name = Mup  
Display = @%systemroot%\system32\drivers\mup.sys, -101  
ImagePath = System32\Drivers\mup.sys  
Type = File system driver  
Start = Boot Start  
Group = Network

Name = NativeWifiP  
Display = NativeWiFi Filter  
ImagePath = system32\DRIVERS\nwifi.sys

## SYSTEM OUTPUT

Type = Kernel driver  
 Start = Manual  
 Group = NDIS

Name = NDIS  
 Display = @%SystemRoot%\system32\drivers\ndis.sys,-200  
 ImagePath = system32\drivers\ndis.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = NDIS Wrapper

Name = NdisTapi  
 Display = @%systemroot%\system32\rascfg.dll,-32001  
 ImagePath = system32\DRIVERS\ndistapi.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = Ndisuio  
 Display = NDIS Usermode I/O Protocol  
 ImagePath = system32\DRIVERS\ndisuio.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = NDIS

Name = NdisWan  
 Display = @%systemroot%\system32\rascfg.dll,-32002  
 ImagePath = system32\DRIVERS\ndiswan.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = NDPProxy  
 Display = NDIS Proxy  
 ImagePath =  
 Type = Kernel driver  
 Start = Manual  
 Group = PNP\_TDI

Name = NetBIOS  
 Display = NetBIOS Interface  
 ImagePath = system32\DRIVERS\netbios.sys  
 Type = File system driver  
 Start = System Start  
 Group = NetBIOSGroup

Name = NetBT  
 Display = @%SystemRoot%\system32\drivers\netbt.sys,-2

## SYSTEM OUTPUT

ImagePath = System32\DRIVERS\netbt.sys  
 Type = Kernel driver  
 Start = System Start  
 Group = PNP\_TDI

Name = NETwNs64  
 Display = \_\_\_ Intel(R) Wireless WiFi Link 5000 Series Adapter Driver for Windows  
 7 - 64 Bit  
 ImagePath = system32\DRIVERS\NETwsw00.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = NDIS

Name = Npfs  
 Display =  
 ImagePath =  
 Type = File system driver  
 Start = System Start  
 Group = File system

Name = nsiproxy  
 Display = @%SystemRoot%\system32\drivers\nsiproxy.sys,-2  
 ImagePath = system32\drivers\nsiproxy.sys  
 Type = Kernel driver  
 Start = System Start  
 Group =

Name = Ntfs  
 Display =  
 ImagePath =  
 Type = File system driver  
 Start = Manual  
 Group = Boot File System

Name = Null  
 Display =  
 ImagePath =  
 Type = Kernel driver  
 Start = System Start  
 Group = Base

Name = nusb3xhc  
 Display = Renesas Electronics USB 3.0 Host Controller Driver  
 ImagePath = \SystemRoot\system32\drivers\nusb3xhc.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Base

## SYSTEM OUTPUT

Name = partmgr  
 Display = @%SystemRoot%\system32\drivers\partmgr.sys, -100  
 ImagePath = System32\drivers\partmgr.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = Boot Bus Extender

Name = pci  
 Display = PCI Bus Driver  
 ImagePath = system32\drivers\pci.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = Boot Bus Extender

Name = pcw  
 Display = Performance Counters for Windows Driver  
 ImagePath = System32\drivers\pcw.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = Base

Name = PEAUTH  
 Display = PEAUTH  
 ImagePath = system32\drivers\peauth.sys  
 Type = Kernel driver  
 Start = Auto Start  
 Group =

Name = PptpMiniport  
 Display = @%systemroot%\system32\rascfg.dll, -32006  
 ImagePath = system32\DRIVERS\raspptp.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = Psched  
 Display = @%SystemRoot%\System32\drivers\pacer.sys, -101  
 ImagePath = system32\DRIVERS\pacer.sys  
 Type = Kernel driver  
 Start = System Start  
 Group = NDIS

Name = RasAgileVpn  
 Display = WAN Miniport (IKEv2)  
 ImagePath = system32\DRIVERS\AgileVpn.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =



## SYSTEM OUTPUT

Name = Rasl2tp  
 Display = @%systemroot%\system32\rascfg.dll, -32005  
 ImagePath = system32\DRIVERS\rasl2tp.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = RasPppoe  
 Display = @%systemroot%\system32\rascfg.dll, -32007  
 ImagePath = system32\DRIVERS\rasppoe.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = RasSstp  
 Display = @%systemroot%\system32\sstpsvc.dll, -202  
 ImagePath = system32\DRIVERS\rassstp.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = rdbss  
 Display = @%systemroot%\system32\wkssvc.dll, -1000  
 ImagePath = system32\DRIVERS\rdbss.sys  
 Type = File system driver  
 Start = System Start  
 Group = Network

Name = rdpbus  
 Display = Remote Desktop Device Redirector Bus Driver  
 ImagePath = \SystemRoot\system32\drivers\rdpbus.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = RDPCDD  
 Display = @%systemroot%\system32\DRIVERS\RDPCDD.sys, -100  
 ImagePath = System32\DRIVERS\RDPCDD.sys  
 Type = Kernel driver  
 Start = System Start  
 Group = Video Save

Name = RDPENCDD  
 Display = @%systemroot%\system32\drivers\RDPENCDD.sys, -101  
 ImagePath = system32\drivers\rdpencdd.sys  
 Type = Kernel driver  
 Start = System Start

## SYSTEM OUTPUT

Group = Video Save

Name = RDPREFMP  
 Display = @%systemroot%\system32\drivers\RdpRefMp.sys, -101  
 ImagePath = system32\drivers\rdprefmp.sys  
 Type = Kernel driver  
 Start = System Start  
 Group = Video Save

Name = rspndr  
 Display = Link-Layer Topology Discovery Responder  
 ImagePath = system32\DRIVERS\rspndr.sys  
 Type = Kernel driver  
 Start = Auto Start  
 Group = NDIS

Name = secdrv  
 Display = Security Driver  
 ImagePath =  
 Type = Kernel driver  
 Start = Disabled  
 Group =

Name = Serenum  
 Display = Serenum Filter Driver  
 ImagePath = system32\DRIVERS\serenum.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = PNP Filter

Name = Serial  
 Display = Serial port driver  
 ImagePath = system32\DRIVERS\serial.sys  
 Type = Kernel driver  
 Start = System Start  
 Group = Extended base

Name = spldr  
 Display = Security Processor Loader Driver  
 ImagePath =  
 Type = Kernel driver  
 Start = Boot Start  
 Group =

Name = srv  
 Display = @%systemroot%\system32\svrsvc.dll, -102  
 ImagePath = System32\DRIVERS\srv.sys  
 Type = File system driver

## SYSTEM OUTPUT

Start = Manual  
Group = Network

Name = srv2  
Display = @%systemroot%\system32\srvsvc.dll,-104  
ImagePath = System32\DRIVERS\srv2.sys  
Type = File system driver  
Start = Manual  
Group = Network

Name = srvnet  
Display =  
ImagePath = System32\DRIVERS\srvnet.sys  
Type = File system driver  
Start = Manual  
Group = Network

Name = storflt  
Display = @%SystemRoot%\system32\vmstorfltres.dll,-1000  
ImagePath = system32\drivers\vmstorfl.sys  
Type = Kernel driver  
Start = Boot Start  
Group = Extended Base

Name = swenum  
Display = Software Bus Driver  
ImagePath = \SystemRoot\system32\drivers\swenum.sys  
Type = Kernel driver  
Start = Manual  
Group =

Name = Tcpip  
Display = @%SystemRoot%\system32\tcpipcfg.dll,-50003  
ImagePath = System32\drivers\tcpip.sys  
Type = Kernel driver  
Start = Boot Start  
Group = PNP\_TDI

Name = tcpipreg  
Display = TCP/IP Registry Compatibility  
ImagePath = System32\drivers\tcpipreg.sys  
Type = Kernel driver  
Start = Auto Start  
Group =

Name = tdx  
Display = @%SystemRoot%\system32\tcpipcfg.dll,-50004  
ImagePath = system32\DRIVERS\tdx.sys

## SYSTEM OUTPUT

Type = Kernel driver  
 Start = System Start  
 Group = PNP\_TDI

Name = TermDD  
 Display = Terminal Device Driver  
 ImagePath = \SystemRoot\system32\drivers\termdd.sys  
 Type = Kernel driver  
 Start = System Start  
 Group =

Name = TPM  
 Display = TPM  
 ImagePath = system32\drivers\tpm.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Boot Bus Extender

Name = tunnel  
 Display = Microsoft Tunnel Miniport Adapter Driver  
 ImagePath = system32\DRIVERS\tunnel.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = NDIS

Name = udfs  
 Display = udfs  
 ImagePath = system32\DRIVERS\udfs.sys  
 Type = File system driver  
 Start = Disabled  
 Group = Boot File System

Name = umbus  
 Display = UMBus Enumerator Driver  
 ImagePath = \SystemRoot\system32\drivers\umbus.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Name = usbehci  
 Display = Microsoft USB 2.0 Enhanced Host Controller Miniport Driver  
 ImagePath = \SystemRoot\system32\drivers\usbehci.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Base

Name = vdrvroot  
 Display = Microsoft Virtual Drive Enumerator Driver

## SYSTEM OUTPUT

ImagePath = system32\drivers\vdrvroot.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = Boot Bus Extender

Name = VgaSave  
 Display =  
 ImagePath = \SystemRoot\System32\drivers\vga.sys  
 Type = Kernel driver  
 Start = System Start  
 Group = Video Save

Name = volmgr  
 Display = Volume Manager Driver  
 ImagePath = system32\drivers\volmgr.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = System Bus Extender

Name = volmgrx  
 Display = @%SystemRoot%\system32\drivers\volmgrx.sys,-100  
 ImagePath = System32\drivers\volmgrx.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = System Bus Extender

Name = volsnap  
 Display = Storage volumes  
 ImagePath = system32\drivers\volsnap.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group =

Name = vwifibus  
 Display = Virtual WiFi Bus Driver  
 ImagePath = system32\DRIVERS\vwifibus.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = vwifflt  
 Display = Virtual WiFi Filter Driver  
 ImagePath = system32\DRIVERS\vwifflt.sys  
 Type = Kernel driver  
 Start = System Start  
 Group = NDIS

Name = Wanarpv6

## SYSTEM OUTPUT

Display = @%systemroot%\system32\rascfg.dll,-32012  
 ImagePath = system32\DRIVERS\wanarp.sys  
 Type = Kernel driver  
 Start = System Start  
 Group =

Name = Wdf01000  
 Display = @%SystemRoot%\system32\drivers\Wdf01000.sys,-1000  
 ImagePath = system32\drivers\Wdf01000.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = WdfLoadGroup

Name = WfpLwf  
 Display = WFP Lightweight Filter  
 ImagePath = system32\DRIVERS\wfpLwf.sys  
 Type = Kernel driver  
 Start = System Start  
 Group = NDIS

Name = WIMMount  
 Display = WIMMount  
 ImagePath = system32\drivers\wimmount.sys  
 Type = File system driver  
 Start = Manual  
 Group = FSFilter Infrastructure

Name = WmiAcpi  
 Display = Microsoft Windows Management Interface for ACPI  
 ImagePath = \SystemRoot\system32\drivers\wmiaapi.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Name = ws2ifsl  
 Display = Windows Socket 2.0 Non-IFS Service Provider Support Environment  
 ImagePath = \SystemRoot\system32\drivers\ws2ifsl.sys  
 Type = Kernel driver  
 Start = System Start  
 Group = PNP\_TDI

Name = WudfPf  
 Display = @%SystemRoot%\system32\drivers\WudfPf.sys,-1000  
 ImagePath = system32\drivers\WudfPf.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = base

## SYSTEM OUTPUT

Tue Apr 19 01:25:12 2016Z

Name = MSK80Service  
 Display = McAfee Anti-Spam Service  
 ImagePath = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"  
 /McCoreSvc  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Tue Apr 19 01:25:10 2016Z

Name = McProxy  
 Display = McAfee Proxy Service  
 ImagePath = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"  
 /McCoreSvc  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Tue Apr 19 01:25:09 2016Z

Name = McNaiAnn  
 Display = McAfee VirusScan Announcer  
 ImagePath = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"  
 /McCoreSvc  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Tue Apr 19 01:25:08 2016Z

Name = McMPFSvc  
 Display = McAfee Personal Firewall Service  
 ImagePath = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"  
 /McCoreSvc  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Tue Apr 19 01:25:06 2016Z

Name = McBootDelayStartSvc  
 Display = McAfee Boot Delay Start Service  
 ImagePath = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"  
 /McCoreSvc  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Tue Apr 19 01:25:05 2016Z

Name = HomeNetSvc  
 Display = McAfee Home Network

## SYSTEM OUTPUT

ImagePath = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"  
/McCoreSvc

Type = Share\_Process  
Start = Auto Start  
Group =

Tue Apr 19 01:25:04 2016Z

Name = McAPExe  
Display = McAfee AP Service  
ImagePath = "C:\Program Files\McAfee\MSC\McAPExe.exe"  
Type = Own\_Process  
Start = Auto Start  
Group =

Tue Apr 19 01:25:03 2016Z

Name = mfefire  
Display = McAfee Firewall Core Service  
ImagePath = "C:\Program Files\Common Files\McAfee\SystemCore\mfefire.exe"  
Type = Own\_Process  
Start = Manual  
Group =

Tue Apr 19 01:25:00 2016Z

Name = mfevtp  
Display = McAfee Validation Trust Protection Service  
ImagePath = "C:\Windows\system32\mfevtps.exe"  
Type = Own\_Process  
Start = Manual  
Group =

Tue Apr 19 01:22:11 2016Z

Name = McAfee SiteAdvisor Service  
Display = McAfee SiteAdvisor Service  
ImagePath = "C:\Program Files (x86)\McAfee\SiteAdvisor\McSACore.exe"  
Type = Own\_Process  
Start = Auto Start  
Group =

Tue Apr 19 01:21:52 2016Z

Name = mcpltsvc  
Display = McAfee Platform Services  
ImagePath = "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"  
/McCoreSvc  
Type = Share\_Process  
Start = Auto Start  
Group =

Tue Apr 19 01:21:37 2016Z



## SYSTEM OUTPUT

Name = PEFService  
 Display = Intel Security PEF Service  
 ImagePath = "C:\Program Files\Common Files\Intel Security\PEF\CORE\PEFService.exe"  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

Tue Apr 19 01:21:20 2016Z

Name = mccspsvc  
 Display = McAfee CSP Service  
 ImagePath = "C:\Program Files\Common  
 Files\McAfee\CSP\1.8.267.0\McCSPServiceHost.exe"  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

Sat Apr 16 22:47:57 2016Z

Name = MSPQM  
 Display = Microsoft Streaming Quality Manager Proxy  
 ImagePath = system32\drivers\MSPQM.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Wed Apr 13 11:43:26 2016Z

Name = TrustedInstaller  
 Display = @%SystemRoot%\servicing\TrustedInstaller.exe,-100  
 ImagePath = %SystemRoot%\servicing\TrustedInstaller.exe  
 Type = Own\_Process  
 Start = Manual  
 Group = ProfSvc\_Group

Wed Apr 6 14:20:46 2016Z

Name = USBSTOR  
 Display = USB Mass Storage Driver  
 ImagePath = system32\DRIVERS\USBSTOR.SYS  
 Type = Kernel driver  
 Start = Manual  
 Group =

Sun Mar 27 00:31:42 2016Z

Name = MBAMScheduler  
 Display =  
 ImagePath = "C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamscheduler.exe"  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

## SYSTEM OUTPUT

Sun Mar 27 00:31:41 2016Z

Name = MBAMService  
 Display =  
 ImagePath = "C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamservice.exe"  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

Thu Mar 10 19:38:21 2016Z

Name = Netaapl  
 Display = Apple Mobile Device Ethernet Service  
 ImagePath = system32\DRIVERS\netaapl64.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = NDIS

Name = USBAAPL64  
 Display = Apple Mobile USB Driver  
 ImagePath = System32\Drivers\usbaapl64.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Base

Thu Feb 25 02:16:29 2016Z

Name = usbaudio  
 Display = USB Audio Driver (WDM)  
 ImagePath = system32\drivers\usbaudio.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Sun Feb 21 00:01:18 2016Z

Name = WinDefend  
 Display = @%ProgramFiles%\Windows Defender\MsMpRes.dll,-103  
 ImagePath = %SystemRoot%\System32\svchost.exe -k secsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group =

Sun Feb 14 15:57:33 2016Z

Name = drmkaud  
 Display = Microsoft Trusted Audio Drivers  
 ImagePath = \SystemRoot\system32\drivers\drmkaud.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = MSKSSRV

## SYSTEM OUTPUT

Display = Microsoft Streaming Service Proxy  
 ImagePath = system32\drivers\MSKSSRV.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Name = MSPCLOCK  
 Display = Microsoft Streaming Clock Proxy  
 ImagePath = system32\drivers\MSPCLOCK.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Name = MSTEE  
 Display = Microsoft Streaming Tee/Sink-to-Sink Converter  
 ImagePath = system32\drivers\MSTEE.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Wed Feb 10 01:34:39 2016Z

Name = tap0901  
 Display = TAP-Windows Adapter V9  
 ImagePath = system32\DRIVERS\tap0901.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = NDIS

Tue Feb 9 22:07:39 2016Z

Name = clr\_optimization\_v2.0.50727\_32  
 Display = Microsoft .NET Framework NGEN v2.0.50727\_X86  
 ImagePath = %systemroot%\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe  
 Type = Own\_Process  
 Start = Disabled  
 Group =

Name = clr\_optimization\_v2.0.50727\_64  
 Display = Microsoft .NET Framework NGEN v2.0.50727\_X64  
 ImagePath = %systemroot%\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe  
 Type = Own\_Process  
 Start = Disabled  
 Group =

Wed Feb 3 04:32:57 2016Z

Name = BITS  
 Display = @%SystemRoot%\system32\qmgr.dll,-1000  
 ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs  
 Type = Share\_Process

## SYSTEM OUTPUT

Start = Auto Start  
Group =

Tue Feb 2 00:31:05 2016Z

Name = BrYNSvc  
Display = BrYNSvc  
ImagePath = "C:\Program Files (x86)\Browny02\BrYNSvc.exe"  
Type = Own\_Process  
Start = Manual  
Group =

Tue Feb 2 00:20:01 2016Z

Name = PDFProFiltSrvPP  
Display = PDFProFiltSrvPP  
ImagePath = C:\Program Files (x86)\Nuance\PaperPort\PDFProFiltSrvPP.exe  
Type = Own\_Process  
Start = Auto Start  
Group =

Mon Feb 1 03:04:18 2016Z

Name = StillCam  
Display = Still Serial Digital Camera Driver  
ImagePath = system32\DRIVERS\serscan.sys  
Type = Kernel driver  
Start = Manual  
Group = Base

Tue Jan 19 22:34:35 2016Z

Name = IntuitUpdateServiceV4  
Display = Intuit Update Service v4  
ImagePath = "C:\Program Files (x86)\Common Files\Intuit\Update Service  
v4\IntuitUpdateService.exe"  
Type = Own\_Process  
Start = Auto Start  
Group =

Tue Jan 19 22:14:22 2016Z

Name = msiserver  
Display = @%SystemRoot%\system32\msimsg.dll,-27  
ImagePath = %systemroot%\system32\msiexec.exe /V  
Type = Own\_Process  
Start = Auto Start  
Group =

Thu Jan 7 22:15:30 2016Z

Name = iPod Service  
Display = iPod Service  
ImagePath = "C:\Program Files\iPod\bin\iPodService.exe"

## SYSTEM OUTPUT

Type = Own\_Process  
 Start = Manual  
 Group =

Thu Jan 7 22:11:07 2016Z

Name = Bonjour Service  
 Display = Bonjour Service  
 ImagePath = "C:\Program Files\Bonjour\mDNSResponder.exe"  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

Fri Jan 1 20:52:19 2016Z

Name = MozillaMaintenance  
 Display = Mozilla Maintenance Service  
 ImagePath = "C:\Program Files (x86)\Mozilla Maintenance  
 Service\maintenanceservice.exe"  
 Type = Own\_Process  
 Start = Manual  
 Group =

Sat Nov 28 20:21:16 2015Z

Name = {1BDD94C3-9D85-46F0-87E3-BD3288A5F6BD}  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Wed Nov 11 20:31:53 2015Z

Name = SharedAccess  
 Display = @%SystemRoot%\system32\ipnathlp.dll, -106  
 ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group =

Wed Nov 11 20:31:50 2015Z

Name = {A9E50A43-973B-4CAD-B78E-EA0321A4A293}  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Mon Oct 19 23:21:21 2015Z

Name = MSDTC Bridge 4.0.0.0  
 Display =

## SYSTEM OUTPUT

ImagePath =  
 Type =  
 Start =  
 Group =

Name = SMSvcHost 4.0.0.0  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = Windows Workflow Foundation 4.0.0.0  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Fri Oct 2 14:28:51 2015Z

Name = McODS  
 Display = McAfee Scanner  
 ImagePath = "C:\Program Files\McAfee\VirusScan\mcods.exe"  
 Type = Own\_Process  
 Start = Manual  
 Group =

Wed Sep 23 03:20:38 2015Z

Name = usbvideo  
 Display = USB Video Device (WDM)  
 ImagePath = System32\Drivers\usbvideo.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Sat Sep 12 00:14:59 2015Z

Name = ASP.NET  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Sat Sep 12 00:14:57 2015Z

Name = ASP.NET\_4.0.30319  
 Display =  
 ImagePath =  
 Type =

## SYSTEM OUTPUT

Start =  
Group =

Name = aspnet\_state  
Display = ASP.NET State Service  
ImagePath = %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\aspnet\_state.exe  
Type = Own\_Process  
Start = Disabled  
Group =

Sat Sep 12 00:14:30 2015Z

Name = NetMsmqActivator  
Display =  
@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll, -8195  
ImagePath = "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe"  
-NetMsmqActivator  
Type = Share\_Process  
Start = Disabled  
Group =

Sat Sep 12 00:14:29 2015Z

Name = NetPipeActivator  
Display =  
@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll, -8197  
ImagePath = C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe  
Type = Share\_Process  
Start = Disabled  
Group =

Sat Sep 12 00:14:25 2015Z

Name = NetTcpActivator  
Display =  
@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll, -8199  
ImagePath = C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe  
Type = Share\_Process  
Start = Disabled  
Group =

Sat Sep 12 00:14:23 2015Z

Name = NetTcpPortSharing  
Display =  
@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceModelInstallRC.dll, -8201  
ImagePath = C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe  
Type = Share\_Process  
Start = Disabled  
Group =

Sat Sep 12 00:14:19 2015Z

## SYSTEM OUTPUT

Name = .NET Memory Cache 4.0  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Sat Sep 12 00:09:28 2015Z

Name = stisvc  
 Display = @%SystemRoot%\system32\wiaservc.dll,-9  
 ImagePath = %SystemRoot%\system32\svchost.exe -k imgsvc  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

Fri Sep 11 18:30:16 2015Z

Name = Apple Mobile Device  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Fri Sep 11 17:57:59 2015Z

Name = Apple Mobile Device Service  
 Display = Apple Mobile Device Service  
 ImagePath = "C:\Program Files\Common Files\Apple\Mobile Device  
 Support\AppleMobileDeviceService.exe"  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

Fri Sep 11 14:56:27 2015Z

Name = gupdate  
 Display = Google Update Service (gupdate)  
 ImagePath = "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /svc  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

Name = gupdatem  
 Display = Google Update Service (gupdatem)  
 ImagePath = "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /medsvc  
 Type = Own\_Process  
 Start = Manual  
 Group =

Fri Sep 11 07:47:27 2015Z



## SYSTEM OUTPUT

Name = WbioSrvc  
 Display = @%systemroot%\system32\wbiosrv.dll,-100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k WbioSvcGroup  
 Type = Share\_Process  
 Start = Manual  
 Group = SmartCardGroup

Thu Sep 10 21:49:02 2015Z

Name = clr\_optimization\_v4.0.30319\_64  
 Display = Microsoft .NET Framework NGEN v4.0.30319\_X64  
 ImagePath = C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

Thu Sep 10 21:49:01 2015Z

Name = clr\_optimization\_v4.0.30319\_32  
 Display = Microsoft .NET Framework NGEN v4.0.30319\_X86  
 ImagePath = C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

Thu Sep 10 21:48:06 2015Z

Name = .NET CLR Networking 4.0.0.0  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Thu Sep 10 21:30:14 2015Z

Name = eventlog  
 Display = @%SystemRoot%\system32\wevtsvc.dll,-200  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted  
 Type = Share\_Process  
 Start = Auto Start  
 Group = Event Log

Name = Outlook  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Thu Sep 10 21:28:37 2015Z

Name = ospsv

## SYSTEM OUTPUT

Display = Office Software Protection Platform  
 ImagePath = "C:\Program Files\Common Files\Microsoft  
 Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE"

Type = Own\_Process  
 Start = Manual  
 Group =

Thu Sep 10 20:46:43 2015Z

Name = DiagTrack  
 Display = @%SystemRoot%\system32\UtcResources.dll,-3001  
 ImagePath = %SystemRoot%\System32\svchost.exe -k utcsvc  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

Thu Sep 10 19:42:05 2015Z

Name = ose  
 Display = Office Source Engine  
 ImagePath = "C:\Program Files (x86)\Common Files\Microsoft Shared\Source  
 Engine\OSE.EXE"  
 Type = Own\_Process  
 Start = Manual  
 Group =

Thu Sep 10 17:10:15 2015Z

Name = IKEEXT  
 Display = @%SystemRoot%\system32\ikeext.dll,-501  
 ImagePath = %systemroot%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Thu Sep 10 17:09:34 2015Z

Name = HipShieldK  
 Display = McAfee Inc. HipShieldK  
 ImagePath = system32\drivers\HipShieldK.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Thu Sep 10 16:33:32 2015Z

Name = odserv  
 Display = Microsoft Office Diagnostics Service  
 ImagePath = "C:\Program Files (x86)\Common Files\Microsoft  
 Shared\OFFICE12\ODSERV.EXE"  
 Type = Own\_Process  
 Start = Manual  
 Group =

## SYSTEM OUTPUT

Thu Sep 10 04:09:03 2015Z

Name = WMPNetworkSvc  
 Display = @%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe, -101  
 ImagePath = "%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe"  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

Thu Sep 10 04:09:02 2015Z

Name = HomeGroupListener  
 Display = @%SystemRoot%\System32\ListSvc.dll, -100  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Manual  
 Group =

Thu Sep 10 04:08:46 2015Z

Name = FDResPub  
 Display = @%systemroot%\system32\fdrespub.dll, -100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Thu Sep 3 18:12:30 2015Z

Name = WSearch  
 Display = @%systemroot%\system32\SearchIndexer.exe, -103  
 ImagePath = %systemroot%\system32\SearchIndexer.exe /Embedding  
 Type = Own\_Process  
 Start = Auto Start  
 Group =

Thu Sep 3 17:49:58 2015Z

Name = CertPropSvc  
 Display = @%SystemRoot%\System32\certprop.dll, -11  
 ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Name = SCardSvr  
 Display = @%SystemRoot%\System32\SCardSvr.dll, -1  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation  
 Type = Share\_Process  
 Start = Auto Start  
 Group = SmartCardGroup

## SYSTEM OUTPUT

Thu Sep 3 17:49:37 2015Z

Name = {720B974A-3E6B-42BF-9839-4EE6CD676477}  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Fri Feb 20 18:42:20 2015Z

Name = adp94xx  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\adp94xx.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = adpahci  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\adpahci.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = adpu320  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\adpu320.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = aliide  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\aliide.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = System Bus Extender

Name = amdide  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\amdide.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = System Bus Extender

Name = amdsata  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\amdsata.sys  
 Type = Kernel driver

## SYSTEM OUTPUT

Start = Manual  
Group = SCSI miniport

Name = amdsbs  
Display =  
ImagePath = \SystemRoot\system32\drivers\amdsbs.sys  
Type = Kernel driver  
Start = Manual  
Group = SCSI Miniport

Name = arc  
Display =  
ImagePath = \SystemRoot\system32\drivers\arc.sys  
Type = Kernel driver  
Start = Manual  
Group = SCSI Miniport

Name = arcsas  
Display =  
ImagePath = \SystemRoot\system32\drivers\arcsas.sys  
Type = Kernel driver  
Start = Manual  
Group = SCSI miniport

Name = cmdide  
Display =  
ImagePath = \SystemRoot\system32\drivers\cmdide.sys  
Type = Kernel driver  
Start = Manual  
Group = System Bus Extender

Name = elxstor  
Display =  
ImagePath = \SystemRoot\system32\drivers\elxstor.sys  
Type = Kernel driver  
Start = Manual  
Group = SCSI Miniport

Name = HpSAMD  
Display =  
ImagePath = \SystemRoot\system32\drivers\HpSAMD.sys  
Type = Kernel driver  
Start = Manual  
Group = SCSI Miniport

Name = iaStorV  
Display =  
ImagePath = \SystemRoot\system32\drivers\iaStorV.sys

## SYSTEM OUTPUT

Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = iirsp  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\iirsp.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = intelide  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\intelide.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = System Bus Extender

Name = isapnp  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\isapnp.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Boot Bus Extender

Name = LSI\_FC  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\lsi\_fc.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = LSI\_SAS  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\lsi\_sas.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = LSI\_SAS2  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\lsi\_sas2.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = LSI\_SCSI  
 Display =

## SYSTEM OUTPUT

ImagePath = \SystemRoot\system32\drivers\lsi\_scsi.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = megasas  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\megasas.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = MegaSR  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\MegaSR.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = mpio  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\mpio.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Boot Bus Extender

Name = msdsm  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\msdsm.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = System Bus Extender

Name = nfrd960  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\nfrd960.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = nvraid  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\nvraid.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = System Bus Extender

Name = nvstor

## SYSTEM OUTPUT

Display =  
 ImagePath = \SystemRoot\system32\drivers\nvstor.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = pciide  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\pciide.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = System Bus Extender

Name = ql2300  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\ql2300.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = ql40xx  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\ql40xx.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = sbp2port  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\sbp2port.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = SiSRaid2  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\SiSRaid2.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = SiSRaid4  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\sisraid4.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport



## SYSTEM OUTPUT

Name = stexstor  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\stexstor.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = storvsc  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\storvsc.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Base

Name = viaide  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\viaide.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = System Bus Extender

Name = vmbus  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\vmbus.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = System Bus Extender

Name = vsmraid  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\vsmraid.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI Miniport

Name = wd  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\wd.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Fri Feb 20 18:42:17 2015Z

Name = EapHost  
 Display = @%systemroot%\system32\eapsvc.dll, -1  
 ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual

## SYSTEM OUTPUT

Group =

Name = terminpt  
 Display = Microsoft Remote Desktop Input Driver  
 ImagePath = \SystemRoot\system32\drivers\terminpt.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Name = TsUsbGD  
 Display = Remote Desktop Generic USB Device  
 ImagePath = \SystemRoot\system32\drivers\TsUsbGD.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Fri Feb 20 18:23:16 2015Z

Name = cphs  
 Display = Intel(R) Content Protection HECI Service  
 ImagePath = %SystemRoot%\SysWow64\IntelCpHeciSvc.exe  
 Type = Own\_Process  
 Start = Manual  
 Group =

Fri Feb 20 18:22:35 2015Z

Name = {FD2B5103-617C-4AE6-8DC4-A4772C463DDC}  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Fri Feb 20 17:05:34 2015Z

Name = vcsFPSservice  
 Display = Validity VCS Fingerprint Service  
 ImagePath = C:\Windows\system32\vcsFPSservice.exe  
 Type = Own\_Process  
 Start = Auto Start  
 Group = ValiditySensors

Fri Feb 20 16:54:33 2015Z

Name = AtiHDAudioService  
 Display = AMD Function Driver for HD Audio Service  
 ImagePath = system32\drivers\AtihdW76.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

## SYSTEM OUTPUT

Fri Feb 20 16:54:27 2015Z

Name = amdkmdap  
 Display =  
 ImagePath = system32\DRIVERS\atikmpag.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Video

Fri Feb 20 16:54:14 2015Z

Name = {3ED9F155-8201-430C-85E1-EDD7020DE0CF}  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Fri Feb 20 16:53:55 2015Z

Name = AMD External Events Utility  
 Display =  
 ImagePath = %SystemRoot%\system32\atiesrxx.exe  
 Type = Own\_Process  
 Start = Auto Start  
 Group = Event log

Name = Atierecord  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Fri Feb 20 16:53:49 2015Z

Name = {8B32CCEF-F092-453D-A04B-084246668014}  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Fri Feb 20 16:53:43 2015Z

Name = {749B2830-EBF4-4268-8BFD-189D3224ACFB}  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Fri Feb 20 16:53:35 2015Z

## SYSTEM OUTPUT

Name = hpsrv  
 Display = HP Service  
 ImagePath = %SystemRoot%\system32\Hpsservice.exe  
 Type = Own\_Process  
 Start = Auto Start  
 Group = UIGroup

Fri Feb 20 16:53:06 2015Z

Name = ohci1394  
 Display = 1394 OHCI Compliant Host Controller (Legacy)  
 ImagePath = \SystemRoot\system32\drivers\ohci1394.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Mon Dec 1 14:38:46 2014Z

Name = SysMain  
 Display = @%SystemRoot%\system32\sysmain.dll,-1000  
 ImagePath = %systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Mon Dec 1 14:16:45 2014Z

Name = WatAdminSvc  
 Display = @%SystemRoot%\system32\Wat\WatUX.exe,-601  
 ImagePath = %SystemRoot%\system32\Wat\WatAdminSvc.exe  
 Type = Own\_Process  
 Start = Manual  
 Group =

Mon Dec 1 14:14:27 2014Z

Name = gpsvc  
 Display = @gpapi.dll,-112  
 ImagePath = %windir%\system32\svchost.exe -k GPSvcGroup  
 Type = Own\_Process  
 Start = Auto Start  
 Group = ProfSvc\_Group

Mon Dec 1 14:13:22 2014Z

Name = IEEtwCollectorService  
 Display = @%SystemRoot%\system32\ieetwcollectorres.dll,-1000  
 ImagePath = %SystemRoot%\system32\IEEtwCollector.exe /V  
 Type = Own\_Process  
 Start = Manual  
 Group =

Name = RDPUDD

## SYSTEM OUTPUT

Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = RdpVideoMiniport  
 Display = Remote Desktop Video Miniport Driver  
 ImagePath = System32\drivers\rdpvideominiport.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Mon Dec 1 14:01:16 2014Z

Name = MSDTC Bridge 3.0.0.0  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = ServiceModelEndpoint 3.0.0.0  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = ServiceModelOperation 3.0.0.0  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = ServiceModelService 3.0.0.0  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = SMSvcHost 3.0.0.0  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

## SYSTEM OUTPUT

Name = Windows Workflow Foundation 3.0.0.0  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Mon Dec 1 13:04:59 2014Z

Name = wuauerv  
 Display = @%systemroot%\system32\wuaueng.dll,-105  
 ImagePath = %systemroot%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Mon Dec 1 12:59:32 2014Z

Name = BTHPORT  
 Display = Bluetooth Port Driver  
 ImagePath = System32\Drivers\BTHport.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = PNP Filter

Mon Dec 1 12:59:19 2014Z

Name = Wlansvc  
 Display = @%SystemRoot%\System32\wlansvc.dll,-257  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Auto Start  
 Group = TDI

Sat Nov 29 16:11:45 2014Z

Name = WebClient  
 Display = @%systemroot%\system32\webclnt.dll,-100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService  
 Type = Share\_Process  
 Start = Manual  
 Group = NetworkProvider

Sat Nov 29 16:07:24 2014Z

Name = wudfsvc  
 Display = @%SystemRoot%\system32\wudfsvc.dll,-1000  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Manual  
 Group = PlugPlay

## SYSTEM OUTPUT

Sat Nov 29 16:06:59 2014Z

Name = FontCache  
 Display = @%systemroot%\system32\FntCache.dll,-100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService  
 Type = Share\_Process  
 Start = Auto Start  
 Group = AudioGroup

Tue Apr 12 08:29:05 2011Z

Name = CscService  
 Display = @%systemroot%\system32\cscsvc.dll,-200  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Auto Start  
 Group = ProfSvc\_Group

Tue Apr 12 08:28:48 2011Z

Name = AppMgmt  
 Display = @appmgmts.dll,-3250  
 ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = ehRecvr  
 Display = @%SystemRoot%\ehome\ehrecvr.exe,-101  
 ImagePath = %systemroot%\ehome\ehRecvr.exe  
 Type = Own\_Process  
 Start = Manual  
 Group =

Name = ehSched  
 Display = @%SystemRoot%\ehome\ehsched.exe,-101  
 ImagePath = %systemroot%\ehome\ehsched.exe  
 Type = Own\_Process  
 Start = Manual  
 Group =

Name = Mcx2Svc  
 Display = @%SystemRoot%\ehome\ehres.dll,-15501  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation  
 Type = Share\_Process  
 Start = Disabled  
 Group =

Name = PeerDistSvc  
 Display = @%SystemRoot%\system32\peerdistsvc.dll,-9000  
 ImagePath = %SystemRoot%\System32\svchost.exe -k PeerDist

## SYSTEM OUTPUT

Type = Share\_Process  
 Start = Manual  
 Group =

Name = RDPDR  
 Display = Terminal Server Device Redirector Driver  
 ImagePath = System32\drivers\rdpdr.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = SensrSvc  
 Display = @%SystemRoot%\System32\sensrsvc.dll,-1000  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = StorSvc  
 Display = @%SystemRoot%\System32\StorSvc.dll,-100  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = UmRdpService  
 Display = @%SystemRoot%\system32\umrdp.dll,-1000  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Manual  
 Group =

Tue Apr 12 08:27:52 2011Z

Name = dmvc  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\dmvc.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = s3cap  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\vm3cap.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Video

Name = VMBusHID



## SYSTEM OUTPUT

Display =  
 ImagePath = \SystemRoot\system32\drivers\VMBusHID.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Sun Nov 21 03:58:24 2010Z

Name = BTHMODEM  
 Display = Bluetooth Serial Communications Driver  
 ImagePath = \SystemRoot\system32\drivers\bthmodem.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Sun Nov 21 03:58:22 2010Z

Name = gagp30kx  
 Display = Microsoft Generic AGPv3.0 Filter for K8 Processor Platforms  
 ImagePath = \SystemRoot\system32\drivers\gagp30kx.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = PnP Filter

Name = uagp35  
 Display = Microsoft AGPv3.5 Filter  
 ImagePath = \SystemRoot\system32\drivers\uagp35.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = PnP Filter

Sun Nov 21 03:58:21 2010Z

Name = b06bdrv  
 Display = Broadcom NetXtreme II VBD  
 ImagePath = \SystemRoot\system32\drivers\bxbvda.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = base

Name = HidBth  
 Display = Microsoft Bluetooth HID Miniport  
 ImagePath = \SystemRoot\system32\drivers\hidbth.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = extended base

Sun Nov 21 03:58:19 2010Z

Name = AmdK8  
 Display = AMD K8 Processor Driver  
 ImagePath = \SystemRoot\system32\drivers\amdK8.sys

## SYSTEM OUTPUT

Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Name = AmdPPM  
 Display = AMD Processor Driver  
 ImagePath = \SystemRoot\system32\drivers\amdppm.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Name = Processor  
 Display = Processor Driver  
 ImagePath = \SystemRoot\system32\drivers\processr.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Sun Nov 21 03:58:18 2010Z

Name = ebdrv  
 Display = Broadcom NetXtreme II 10 GigE VBD  
 ImagePath = \SystemRoot\system32\drivers\evbda.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = base

Name = fdc  
 Display = Floppy Disk Controller Driver  
 ImagePath = \SystemRoot\system32\drivers\fdc.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Sun Nov 21 03:58:17 2010Z

Name = pcmcia  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\pcmcia.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = System Bus Extender

Sun Nov 21 03:58:16 2010Z

Name = MTConfig  
 Display = Microsoft Input Configuration Driver  
 ImagePath = \SystemRoot\system32\drivers\MTConfig.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

## SYSTEM OUTPUT

Sun Nov 21 03:58:15 2010Z

Name = circlass  
 Display = Consumer IR Devices  
 ImagePath = \SystemRoot\system32\drivers\circlass.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Sun Nov 21 03:58:13 2010Z

Name = flpydisk  
 Display = Floppy Disk Driver  
 ImagePath = \SystemRoot\system32\drivers\flpydisk.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = sfloppy  
 Display = High-Capacity Floppy Disk Drive  
 ImagePath = \SystemRoot\system32\drivers\sfloppy.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Sun Nov 21 03:58:11 2010Z

Name = HidBatt  
 Display = HID UPS Battery Driver  
 ImagePath = \SystemRoot\system32\drivers\HidBatt.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Sun Nov 21 03:58:08 2010Z

Name = HidIr  
 Display = Microsoft Infrared HID Driver  
 ImagePath = \SystemRoot\system32\drivers\hidir.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = extended base

Sun Nov 21 03:58:07 2010Z

Name = sermouse  
 Display = Serial Mouse Driver  
 ImagePath = \SystemRoot\system32\drivers\sermouse.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Pointer Port

## SYSTEM OUTPUT

Sun Nov 21 03:58:06 2010Z

Name = BrFiltLo  
 Display = Brother USB Mass-Storage Lower Filter Driver  
 ImagePath = \SystemRoot\system32\drivers\BrFiltLo.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = extended base

Name = BrFiltUp  
 Display = Brother USB Mass-Storage Upper Filter Driver  
 ImagePath = \SystemRoot\system32\drivers\BrFiltUp.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = extended base

Sun Nov 21 03:58:05 2010Z

Name = usbohci  
 Display = Microsoft USB Open Host Controller Miniport Driver  
 ImagePath = \SystemRoot\system32\drivers\usbohci.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Base

Name = usbuhci  
 Display = Microsoft USB Universal Host Controller Miniport Driver  
 ImagePath = \SystemRoot\system32\drivers\usbuhci.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Base

Sun Nov 21 03:58:00 2010Z

Name = WacomPen  
 Display = Wacom Serial Pen HID Driver  
 ImagePath = \SystemRoot\system32\drivers\wacompens.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Sun Nov 21 03:57:59 2010Z

Name = crcdisk  
 Display = Crcdisk Filter Driver  
 ImagePath = \SystemRoot\system32\drivers\crcdisk.sys  
 Type = Kernel driver  
 Start = Disabled  
 Group = Pnp Filter

Sun Nov 21 03:57:58 2010Z

Name = UmPass

## SYSTEM OUTPUT

Display = Microsoft UMPass Driver  
 ImagePath = \SystemRoot\system32\drivers\umpass.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Sun Nov 21 03:46:56 2010Z

Name = b57nd60a  
 Display = Broadcom NetXtreme Gigabit Ethernet - NDIS 6.0  
 ImagePath = system32\DRIVERS\b57nd60a.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = NDIS

Name = vga  
 Display =  
 ImagePath = system32\DRIVERS\vgapnp.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Video

Sun Nov 21 03:38:46 2010Z

Name = TsUsbFlt  
 Display =  
 ImagePath = system32\drivers\tsusbflt.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = base

Sun Nov 21 03:33:56 2010Z

Name = SessionEnv  
 Display = @%SystemRoot%\System32\SessEnv.dll,-1026  
 ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group =

Sun Nov 21 03:29:32 2010Z

Name = AcpiPmi  
 Display = ACPI Power Meter Driver  
 ImagePath = \SystemRoot\system32\drivers\acpipmi.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = agp440  
 Display = Intel AGP Bus Filter  
 ImagePath = \SystemRoot\system32\drivers\agp440.sys

## SYSTEM OUTPUT

Type = Kernel driver  
 Start = Manual  
 Group = PnP Filter

Name = amdxtata  
 Display =  
 ImagePath = system32\drivers\amdxtata.sys  
 Type = Kernel driver  
 Start = Boot Start  
 Group = SCSI miniport

Name = ErrDev  
 Display = Microsoft Hardware Error Device Driver  
 ImagePath = \SystemRoot\system32\drivers\errdev.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Name = IPMIDRV  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\IPMIDrv.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = iScsiPrt  
 Display = iScsiPort Driver  
 ImagePath = \SystemRoot\system32\drivers\msiscsi.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = nv\_agp  
 Display = NVIDIA nForce AGP Bus Filter  
 ImagePath = \SystemRoot\system32\drivers\nv\_agp.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = PnP Filter

Name = sffdisk  
 Display = SFF Storage Class Driver  
 ImagePath = \SystemRoot\system32\drivers\sffdisk.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = sffp\_mmc  
 Display = SFF Storage Protocol Driver for MMC

## SYSTEM OUTPUT

ImagePath = \SystemRoot\system32\drivers\sffp\_mmc.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = sffp\_sd  
 Display = SFF Storage Protocol Driver for SDBus  
 ImagePath = \SystemRoot\system32\drivers\sffp\_sd.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = uliagpkx  
 Display = Uli AGP Bus Filter  
 ImagePath = \SystemRoot\system32\drivers\uliagpkx.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = PnP Filter

Name = usbcir  
 Display = eHome Infrared Receiver (USBCIR)  
 ImagePath = \SystemRoot\system32\drivers\usbcir.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Extended Base

Name = vhdmp  
 Display =  
 ImagePath = \SystemRoot\system32\drivers\vhdmp.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = SCSI miniport

Tue Jul 14 04:54:38 2009Z

Name = NdisCap  
 Display = NDIS Capture Lightweight Filter  
 ImagePath = system32\DRIVERS\ndiscap.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = NDIS

Tue Jul 14 04:53:57 2009Z

Name = Smb  
 Display = @%SystemRoot%\system32\tcpipcfg.dll,-50005  
 ImagePath = system32\DRIVERS\smb.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = PNP\_TDI

## SYSTEM OUTPUT

Tue Jul 14 04:53:45 2009Z

Name = TrkWks  
 Display = @%SystemRoot%\system32\trkwks.dll,-1  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Tue Jul 14 04:53:36 2009Z

Name = RpcEptMapper  
 Display = @%windir%\system32\RpcEpMap.dll,-1001  
 ImagePath = %SystemRoot%\system32\svchost.exe -k RPCSS  
 Type = Share\_Process  
 Start = Auto Start  
 Group = COM Infrastructure

Tue Jul 14 04:53:33 2009Z

Name = LanmanServer  
 Display = @%systemroot%\system32\srvsvc.dll,-100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Tue Jul 14 04:53:31 2009Z

Name = LanmanWorkstation  
 Display = @%systemroot%\system32\wkssvc.dll,-100  
 ImagePath = %SystemRoot%\System32\svchost.exe -k NetworkService  
 Type = Share\_Process  
 Start = Auto Start  
 Group = NetworkProvider

Tue Jul 14 04:53:25 2009Z

Name = WmiApRpl  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Tue Jul 14 04:53:24 2009Z

Name = Winmgmt  
 Display = @%Systemroot%\system32\wbem\wmisvc.dll,-205  
 ImagePath = %systemroot%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Auto Start  
 Group =



## SYSTEM OUTPUT

Name = wmiApSrv  
 Display = @%Systemroot%\system32\wbem\wmiapsrv.exe, -110  
 ImagePath = %systemroot%\system32\wbem\WmiApSrv.exe  
 Type = Own\_Process  
 Start = Manual  
 Group =

Tue Jul 14 04:53:21 2009Z

Name = TCPIP6  
 Display = Microsoft IPv6 Protocol Driver  
 ImagePath = system32\DRIVERS\tcpip.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = WANARP  
 Display = @%systemroot%\system32\rascfg.dll, -32011  
 ImagePath = system32\DRIVERS\wanarp.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Tue Jul 14 04:53:20 2009Z

Name = lmhosts  
 Display = @%SystemRoot%\system32\lmhsvc.dll, -101  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted  
 Type = Share\_Process  
 Start = Auto Start  
 Group = TDI

Tue Jul 14 04:53:19 2009Z

Name = Dhcp  
 Display = @%SystemRoot%\system32\dhcpcore.dll, -100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted  
 Type = Share\_Process  
 Start = Auto Start  
 Group = TDI

Name = Winsock  
 Display =  
 ImagePath =  
 Type = 0x0  
 Start = Manual  
 Group =

Tue Jul 14 04:49:48 2009Z

Name = SamSs

## SYSTEM OUTPUT

Display = @%SystemRoot%\system32\samsrv.dll,-1  
 ImagePath = %SystemRoot%\system32\lsass.exe  
 Type = Share\_Process  
 Start = Auto Start  
 Group = MS\_WindowsLocalValidation

Name = W32Time  
 Display = @%SystemRoot%\system32\w32time.dll,-200  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService  
 Type = Share\_Process  
 Start = Manual  
 Group =

Tue Jul 14 04:49:46 2009Z

Name = Dnscache  
 Display = @%SystemRoot%\System32\dnsapi.dll,-101  
 ImagePath = %SystemRoot%\system32\svchost.exe -k NetworkService  
 Type = Share\_Process  
 Start = Auto Start  
 Group = TDI

Tue Jul 14 04:49:45 2009Z

Name = RemoteAccess  
 Display = @%Systemroot%\system32\mprdim.dll,-200  
 ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Disabled  
 Group =

Tue Jul 14 04:49:35 2009Z

Name = RasAuto  
 Display = @%Systemroot%\system32\rasauto.dll,-200  
 ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = RasMan  
 Display = @%Systemroot%\system32\rasmans.dll,-200  
 ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group =

Tue Jul 14 04:49:24 2009Z

Name = DPS  
 Display = @%systemroot%\system32\dps.dll,-500  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceNoNetwork

## SYSTEM OUTPUT

Type = Share\_Process  
 Start = Auto Start  
 Group =

Name = WdiServiceHost  
 Display = @%systemroot%\system32\wdi.dll,-502  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalService  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = WdiSystemHost  
 Display = @%systemroot%\system32\wdi.dll,-500  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Manual  
 Group =

Tue Jul 14 04:49:01 2009Z

Name = .NET CLR Data  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = .NET CLR Networking  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = .NET Data Provider for Oracle  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = .NET Data Provider for SqlServer  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = .NETFramework

## SYSTEM OUTPUT

Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = adsi  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = AeLookupSvc  
 Display = @%SystemRoot%\system32\aelupsvc.dll,-1  
 ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = ALG  
 Display = @%SystemRoot%\system32\Alg.exe,-112  
 ImagePath = %SystemRoot%\System32\alg.exe  
 Type = Own\_Process  
 Start = Manual  
 Group =

Name = AppID  
 Display = @%systemroot%\system32\appidsvc.dll,-102  
 ImagePath = \SystemRoot\system32\drivers\appid.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = AppIDSvc  
 Display = @%systemroot%\system32\appidsvc.dll,-100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation  
 Type = Share\_Process  
 Start = Manual  
 Group = ProfSvc\_Group

Name = Appinfo  
 Display = @%systemroot%\system32\appinfo.dll,-100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group =

## SYSTEM OUTPUT

Name = AudioEndpointBuilder  
 Display = @%SystemRoot%\system32\audiosrv.dll,-204  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Auto Start  
 Group = AudioGroup

Name = AudioSrv  
 Display = @%SystemRoot%\system32\audiosrv.dll,-200  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted  
 Type = Share\_Process  
 Start = Auto Start  
 Group = AudioGroup

Name = AxInstSV  
 Display = @%SystemRoot%\system32\AxInstSV.dll,-103  
 ImagePath = %SystemRoot%\system32\svchost.exe -k AxInstSVGroup  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = BattC  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = BDESVC  
 Display = @%SystemRoot%\system32\bdesvc.dll,-100  
 ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = BFE  
 Display = @%SystemRoot%\system32\bfe.dll,-1001  
 ImagePath = %systemroot%\system32\svchost.exe -k LocalServiceNoNetwork  
 Type = Share\_Process  
 Start = Auto Start  
 Group = NetworkProvider

Name = Browser  
 Display = @%systemroot%\system32\browser.dll,-100  
 ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group = NetworkProvider

## SYSTEM OUTPUT

Name = Brserid  
 Display = Brother MFC Serial Port Interface Driver (WDM)  
 ImagePath = \SystemRoot\System32\Drivers\Brserid.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = BrSerWdm  
 Display = Brother WDM Serial driver  
 ImagePath = \SystemRoot\System32\Drivers\BrSerWdm.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = BrUsbMdm  
 Display = Brother MFC USB Fax Only Modem  
 ImagePath = \SystemRoot\System32\Drivers\BrUsbMdm.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = BrUsbSer  
 Display = Brother MFC USB Serial WDM Driver  
 ImagePath = \SystemRoot\System32\Drivers\BrUsbSer.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = bthserv  
 Display = @%SystemRoot%\System32\bthserv.dll,-101  
 ImagePath = %SystemRoot%\system32\svchost.exe -k bthsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = COMSysApp  
 Display = @comres.dll,-947  
 ImagePath = %SystemRoot%\system32\dllhost.exe  
 /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}  
 Type = Own\_Process  
 Start = Manual  
 Group =

Name = crypt32  
 Display =  
 ImagePath =  
 Type =

## SYSTEM OUTPUT

Start =  
Group =

Name = CryptSvc  
Display = @%SystemRoot%\system32\cryptsvc.dll, -1001  
ImagePath = %SystemRoot%\system32\svchost.exe -k NetworkService  
Type = Share\_Process  
Start = Auto Start  
Group =

Name = DCLocator  
Display =  
ImagePath =  
Type =  
Start =  
Group =

Name = DcomLaunch  
Display = @oleres.dll, -5012  
ImagePath = %SystemRoot%\system32\svchost.exe -k DcomLaunch  
Type = Share\_Process  
Start = Auto Start  
Group = COM Infrastructure

Name = defragsvc  
Display = @%SystemRoot%\system32\defragsvc.dll, -101  
ImagePath = %SystemRoot%\system32\svchost.exe -k defragsvc  
Type = Own\_Process  
Start = Manual  
Group =

Name = dot3svc  
Display = @%systemroot%\system32\dot3svc.dll, -1102  
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted  
Type = Share\_Process  
Start = Manual  
Group = TDI

Name = EFS  
Display = @%SystemRoot%\system32\efssvc.dll, -100  
ImagePath = %SystemRoot%\System32\lsass.exe  
Type = Share\_Process  
Start = Manual  
Group =

Name = ESENT  
Display =  
ImagePath =

## SYSTEM OUTPUT

Type =  
 Start =  
 Group =

Name = EventSystem  
 Display = @comres.dll,-2450  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Name = Fax  
 Display = @%systemroot%\system32\fxsresm.dll,-118  
 ImagePath = %systemroot%\system32\fxssvc.exe  
 Type = Own\_Process  
 Start = Manual  
 Group =

Name = fdPHost  
 Display = @%systemroot%\system32\fdPHost.dll,-100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = Filetrace  
 Display = @%SystemRoot%\system32\drivers\filetrace.sys,-10001  
 ImagePath = system32\drivers\filetrace.sys  
 Type = File system driver  
 Start = Manual  
 Group = FSFilter Activity Monitor

Name = FontCache3.0.0.0  
 Display = @%SystemRoot%\system32\PresentationHost.exe,-3309  
 ImagePath =  
 %systemroot%\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe  
 Type = Own\_Process  
 Start = Manual  
 Group =

Name = FsDepends  
 Display = @%SystemRoot%\system32\drivers\fsdepends.sys,-10001  
 ImagePath = System32\drivers\FsDepends.sys  
 Type = File system driver  
 Start = Manual  
 Group = Filter

Name = hcw85cir



## SYSTEM OUTPUT

```

Display   = Hauppauge Consumer Infrared Receiver
ImagePath = \SystemRoot\system32\drivers\hwc85cir.sys
Type      = Kernel driver
Start     = Manual
Group     = Extended Base

Name      = hidserv
Display   = @%SystemRoot%\System32\hidserv.dll,-101
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Manual
Group     =

Name      = hkmsvc
Display   = @%SystemRoot%\system32\kmsvc.dll,-6
ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
Type      = Share_Process
Start     = Manual
Group     =

Name      = HomeGroupProvider
Display   = @%SystemRoot%\System32\provsvc.dll,-100
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted
Type      = Share_Process
Start     = Manual
Group     =

Name      = idsvc
Display   = @%systemroot%\Microsoft.NET\Framework64\v3.0\Windows Communication
Foundation\ServiceModelInstallRC.dll,-8193
ImagePath = "%systemroot%\Microsoft.NET\Framework64\v3.0\Windows Communication
Foundation\infocard.exe"
Type      = Share_Process
Start     = Manual
Group     =

Name      = inetaccs
Display   =
ImagePath =
Type      =
Start     =
Group     =

Name      = IPBusEnum
Display   = @%systemroot%\system32\IPBusEnum.dll,-102
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted
Type      = Share_Process
Start     = Manual

```

## SYSTEM OUTPUT

Group =

Name = IpFilterDriver  
 Display = @%systemroot%\system32\rascfg.dll,-32013  
 ImagePath = system32\DRIVERS\ipfltdrv.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = iphlpsvc  
 Display = @%SystemRoot%\system32\iphlpvc.dll,-500  
 ImagePath = %SystemRoot%\System32\svchost.exe -k NetSvcs  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Name = IPNAT  
 Display = IP Network Address Translator  
 ImagePath = System32\drivers\ipnat.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = IRENUM  
 Display = @%SystemRoot%\system32\drivers\irenum.sys,-100  
 ImagePath = system32\drivers\irenum.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = KeyIso  
 Display = @keyiso.dll,-100  
 ImagePath = %SystemRoot%\system32\lsass.exe  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = KtmRm  
 Display = @comres.dll,-2946  
 ImagePath = %SystemRoot%\System32\svchost.exe -k NetworkServiceAndNoImpersonation  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = ldap  
 Display =  
 ImagePath =  
 Type =

## SYSTEM OUTPUT

Start =  
Group =

Name = lltdsvc  
Display = @%SystemRoot%\system32\lltdres.dll,-1  
ImagePath = %SystemRoot%\System32\svchost.exe -k LocalService  
Type = Share\_Process  
Start = Manual  
Group =

Name = Lsa  
Display =  
ImagePath =  
Type =  
Start =  
Group =

Name = MMCSS  
Display = @%systemroot%\system32\mmcscs.dll,-100  
ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs  
Type = Share\_Process  
Start = Auto Start  
Group =

Name = MpsSvc  
Display = @%SystemRoot%\system32\FirewallAPI.dll,-23090  
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceNoNetwork  
Type = Share\_Process  
Start = Auto Start  
Group = NetworkProvider

Name = MRxDAV  
Display = @%systemroot%\system32\webclnt.dll,-104  
ImagePath = \SystemRoot\system32\drivers\mrxdav.sys  
Type = File system driver  
Start = Manual  
Group =

Name = MSDTC  
Display = @comres.dll,-2797  
ImagePath = %SystemRoot%\System32\msdtc.exe  
Type = Own\_Process  
Start = Manual  
Group =

Name = mshidkmdf  
Display = @%SystemRoot%\system32\drivers\mshidkmdf.sys,-100  
ImagePath = \SystemRoot\System32\drivers\mshidkmdf.sys

## SYSTEM OUTPUT

Type = Kernel driver  
 Start = Manual  
 Group = Base

Name = MSiSCSI  
 Display = @%SystemRoot%\system32\iscsidsc.dll,-5000  
 ImagePath = %systemroot%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group = iSCSI

Name = MsRPC  
 Display =  
 ImagePath =  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = MSSCNTRS  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = napagent  
 Display = @%SystemRoot%\system32\qagentrt.dll,-6  
 ImagePath = %SystemRoot%\System32\svchost.exe -k NetworkService  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = Netlogon  
 Display = @%SystemRoot%\System32\netlogon.dll,-102  
 ImagePath = %systemroot%\system32\lsass.exe  
 Type = Share\_Process  
 Start = Manual  
 Group = MS\_WindowsRemoteValidation

Name = Netman  
 Display = @%SystemRoot%\system32\netman.dll,-109  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = netprofm  
 Display = @%SystemRoot%\system32\netprofm.dll,-202

## SYSTEM OUTPUT

ImagePath = %SystemRoot%\System32\svchost.exe -k LocalService  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = NlaSvc  
 Display = @%SystemRoot%\System32\nlasvc.dll,-1  
 ImagePath = %SystemRoot%\System32\svchost.exe -k NetworkService  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Name = nsi  
 Display = @%SystemRoot%\system32\nsisvc.dll,-200  
 ImagePath = %systemroot%\system32\svchost.exe -k LocalService  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Name = NTDS  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = p2pimsvc  
 Display = @%SystemRoot%\system32\pnrpsvc.dll,-8004  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServicePeerNet  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = p2psvc  
 Display = @%SystemRoot%\system32\p2psvc.dll,-8006  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServicePeerNet  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = PcaSvc  
 Display = @%SystemRoot%\system32\pcasvc.dll,-1  
 ImagePath = %systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Name = PerfDisk

## SYSTEM OUTPUT

Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = PerfHost  
 Display = @%systemroot%\syswow64\perfhhost.exe, -2  
 ImagePath = %SystemRoot%\SysWow64\perfhhost.exe  
 Type = Own\_Process  
 Start = Manual  
 Group =

Name = PerfNet  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = PerfOS  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = PerfProc  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = pla  
 Display = @%systemroot%\system32\pla.dll, -500  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceNoNetwork  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = PlugPlay  
 Display = @%SystemRoot%\system32\umpnpgmgr.dll, -100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k DcomLaunch  
 Type = Share\_Process  
 Start = Auto Start  
 Group = PlugPlay

## SYSTEM OUTPUT

Name = PNRPAutoReg  
 Display = @%SystemRoot%\system32\pnrpauto.dll,-8002  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServicePeerNet  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = PNRPsvc  
 Display = @%SystemRoot%\system32\pnrpsvc.dll,-8000  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServicePeerNet  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = PolicyAgent  
 Display = @%SystemRoot%\System32\polstore.dll,-5010  
 ImagePath = %SystemRoot%\system32\svchost.exe -k NetworkServiceNetworkRestricted  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = PortProxy  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = Power  
 Display = @%SystemRoot%\system32\umpo.dll,-100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k DcomLaunch  
 Type = Share\_Process  
 Start = Auto Start  
 Group = Plugplay

Name = ProfSvc  
 Display = @%systemroot%\system32\profsvc.dll,-300  
 ImagePath = %systemroot%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Auto Start  
 Group = profsvc\_group

Name = ProtectedStorage  
 Display = @%systemroot%\system32\psbase.dll,-300  
 ImagePath = %SystemRoot%\system32\lsass.exe  
 Type = Share\_Process  
 Start = Manual  
 Group =

## SYSTEM OUTPUT

Name = QWAVE  
 Display = @%SystemRoot%\system32\qwave.dll,-1  
 ImagePath = %windir%\system32\svchost.exe -k LocalServiceAndNoImpersonation  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = QWAVEdrv  
 Display = @%SystemRoot%\system32\drivers\qwavedrv.sys,-1  
 ImagePath = \SystemRoot\system32\drivers\qwavedrv.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = RasAcD  
 Display = Remote Access Auto Connection Driver  
 ImagePath = System32\DRIVERS\rasacd.sys  
 Type = Kernel driver  
 Start = Manual  
 Group = Streams Drivers

Name = RDPDD  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = RDPNP  
 Display = @%systemroot%\system32\drprov.dll,-100  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = RDPWD  
 Display = RDP Winstation Driver  
 ImagePath =  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = RemoteRegistry  
 Display = @regsvc.dll,-1  
 ImagePath = %SystemRoot%\system32\svchost.exe -k regsvc  
 Type = Share\_Process  
 Start = Manual



## SYSTEM OUTPUT

Group =

Name = RpcLocator  
 Display = @%systemroot%\system32\Locator.exe,-2  
 ImagePath = %SystemRoot%\system32\locator.exe  
 Type = Own\_Process  
 Start = Manual  
 Group =

Name = RpcSs  
 Display = @Oleres.dll,-5010  
 ImagePath = %SystemRoot%\system32\svchost.exe -k rpcss  
 Type = Share\_Process  
 Start = Auto Start  
 Group = COM Infrastructure

Name = Schedule  
 Display = @%SystemRoot%\system32\schedsvc.dll,-100  
 ImagePath = %systemroot%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Auto Start  
 Group = SchedulerGroup

Name = SCPolicySvc  
 Display = @%SystemRoot%\System32\certprop.dll,-13  
 ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = SDRSVC  
 Display = @%SystemRoot%\system32\sdrsvc.dll,-107  
 ImagePath = %SystemRoot%\system32\svchost.exe -k SDRSVC  
 Type = Own\_Process  
 Start = Manual  
 Group =

Name = seclogon  
 Display = @%SystemRoot%\system32\seclogon.dll,-7001  
 ImagePath = %windir%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = SENS  
 Display = @%SystemRoot%\system32\Sens.dll,-200  
 ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs  
 Type = Share\_Process

## SYSTEM OUTPUT

Start = Auto Start  
Group = ProfSvc\_Group

Name = ShellHWDetection  
Display = @%SystemRoot%\System32\shsvcs.dll,-12288  
ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs  
Type = Share\_Process  
Start = Auto Start  
Group = ShellSvcGroup

Name = SNMPTRAP  
Display = @%SystemRoot%\system32\snmptrap.exe,-3  
ImagePath = %SystemRoot%\System32\snmptrap.exe  
Type = Own\_Process  
Start = Manual  
Group =

Name = Spooler  
Display = @%systemroot%\system32\spoolsv.exe,-1  
ImagePath = %SystemRoot%\System32\spoolsv.exe  
Type = 0x0  
Start = Auto Start  
Group = SpoolerGroup

Name = sppsvc  
Display = @%SystemRoot%\system32\sppsvc.exe,-101  
ImagePath = %SystemRoot%\system32\sppsvc.exe  
Type = Own\_Process  
Start = Auto Start  
Group =

Name = sppuinotify  
Display = @%SystemRoot%\system32\sppuinotify.dll,-103  
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService  
Type = Share\_Process  
Start = Manual  
Group =

Name = SSDPSRV  
Display = @%systemroot%\system32\ssdpsrv.dll,-100  
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation  
Type = Share\_Process  
Start = Manual  
Group =

Name = SstpSvc  
Display = @%SystemRoot%\system32\sstpsvc.dll,-200  
ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService

## SYSTEM OUTPUT

Type = Share\_Process  
 Start = Manual  
 Group =

Name = swprv  
 Display = @%SystemRoot%\System32\swprv.dll,-103  
 ImagePath = %SystemRoot%\System32\svchost.exe -k swprv  
 Type = Own\_Process  
 Start = Manual  
 Group =

Name = TabletInputService  
 Display = @%SystemRoot%\system32\TabSvc.dll,-100  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Manual  
 Group = PlugPlay

Name = TapiSrv  
 Display = @%SystemRoot%\system32\tapisrv.dll,-10100  
 ImagePath = %SystemRoot%\System32\svchost.exe -k NetworkService  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = TCPIP6TUNNEL  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = TCPIPTUNNEL  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = TDPIPE  
 Display = TDPIPE  
 ImagePath = system32\drivers\tdpipe.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = TDTCP  
 Display = TDTCP

## SYSTEM OUTPUT

ImagePath = system32\drivers\tdtcp.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = TermService  
 Display = @%SystemRoot%\System32\termsrv.dll,-268  
 ImagePath = %SystemRoot%\System32\svchost.exe -k NetworkService  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = Themes  
 Display = @%SystemRoot%\System32\themeservice.dll,-8192  
 ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Auto Start  
 Group = ProfSvc\_Group

Name = THREADORDER  
 Display = @%systemroot%\system32\mmcscs.dll,-102  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = TSDDD  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = tssecsrv  
 Display = @%SystemRoot%\System32\DRIVERS\tssecsrv.sys,-101  
 ImagePath = System32\DRIVERS\tssecsrv.sys  
 Type = Kernel driver  
 Start = Manual  
 Group =

Name = UGatherer  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = UGTHRSVC

## SYSTEM OUTPUT

Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = UI0Detect  
 Display = @%SystemRoot%\system32\ui0detect.exe, -101  
 ImagePath = %SystemRoot%\system32\UI0Detect.exe  
 Type = 0x0  
 Start = Manual  
 Group =

Name = upnphost  
 Display = @%systemroot%\system32\upnphost.dll, -213  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = UxSms  
 Display = @%SystemRoot%\system32\dwm.exe, -2000  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Auto Start  
 Group = UIGroup

Name = VaultSvc  
 Display = @%SystemRoot%\system32\vaultsvc.dll, -1003  
 ImagePath = %SystemRoot%\system32\lsass.exe  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = vds  
 Display = @%SystemRoot%\system32\vds.exe, -100  
 ImagePath = %SystemRoot%\System32\vds.exe  
 Type = Own\_Process  
 Start = Manual  
 Group =

Name = VSS  
 Display = @%systemroot%\system32\vssvc.exe, -102  
 ImagePath = %systemroot%\system32\vssvc.exe  
 Type = Own\_Process  
 Start = Manual  
 Group =

## SYSTEM OUTPUT

Name = W3SVC  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = wbengine  
 Display = @%systemroot%\system32\wbengine.exe, -104  
 ImagePath = "%systemroot%\system32\wbengine.exe"  
 Type = Own\_Process  
 Start = Manual  
 Group =

Name = wncscvc  
 Display = @%SystemRoot%\system32\wncscvc.dll, -3  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceAndNoImpersonation  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = WcsPlugInService  
 Display = @%SystemRoot%\system32\WcsPlugInService.dll, -200  
 ImagePath = %SystemRoot%\system32\svchost.exe -k wcssvc  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = Wecsvc  
 Display = @%SystemRoot%\system32\wecsvc.dll, -200  
 ImagePath = %SystemRoot%\system32\svchost.exe -k NetworkService  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = wercplsupport  
 Display = @%SystemRoot%\System32\wercplsupport.dll, -101  
 ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = WerSvc  
 Display = @%SystemRoot%\System32\wersvc.dll, -100  
 ImagePath = %SystemRoot%\System32\svchost.exe -k WerSvcGroup  
 Type = Share\_Process  
 Start = Manual  
 Group =

## SYSTEM OUTPUT

Name = WinHttpAutoProxySvc  
 Display = @%SystemRoot%\system32\winhttp.dll,-100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalService  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = WinRM  
 Display = @%Systemroot%\system32\wsmsvc.dll,-101  
 ImagePath = %SystemRoot%\System32\svchost.exe -k NetworkService  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = WinSock2  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

Name = WPCSvc  
 Display = @%SystemRoot%\system32\wpcsvc.dll,-100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = WPDBusEnum  
 Display = @%SystemRoot%\system32\wpdbusenum.dll,-100  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted  
 Type = Share\_Process  
 Start = Manual  
 Group =

Name = wscsvc  
 Display = @%SystemRoot%\System32\wscsvc.dll,-200  
 ImagePath = %SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted  
 Type = Share\_Process  
 Start = Auto Start  
 Group =

Name = WSearchIdxPi  
 Display =  
 ImagePath =  
 Type =  
 Start =

## SYSTEM OUTPUT

Group =

Name = WwanSvc  
 Display = @%SystemRoot%\System32\wwansvc.dll,-257  
 ImagePath = %SystemRoot%\system32\svchost.exe -k LocalServiceNoNetwork  
 Type = Share\_Process  
 Start = Manual  
 Group = TDI

Name = xmlprov  
 Display =  
 ImagePath =  
 Type =  
 Start =  
 Group =

-----  
 shares v.20140730  
 (System) Get list of shares from System hive file  
 subkey not found.

-----  
 shutdown v.20080324  
 (System) Gets ShutdownTime value from System hive  
 ControlSet001\Control\Windows key, ShutdownTime value  
 ControlSet001\Control\Windows  
 LastWrite Time Wed Apr 20 02:36:16 2016 (UTC)  
 ShutdownTime = Wed Apr 20 02:36:16 2016 (UTC)

-----  
 shutdowncount v.20080709  
 (System) Retrieves ShutDownCount value  
 ControlSet001\Control\Watchdog\Display not found.

-----  
 stillimage v.20100222  
 (System) Get info on StillImage devices

StillImage Logging Level  
 STICLI Logging Level = 0x4  
 STIMON Logging Level = 0x4

-----  
 svc v.20131010  
 (System) Lists Services key contents by LastWrite time (CSV)

Time,Name,DisplayName,ImagePath/ServiceDll,Type,Start,ObjectName



## SYSTEM OUTPUT

Wed Apr 20 02:39:31 2016  
 Z,AsyncMac,@%systemroot%\system32\rascfg.dll;-32000,system32\DRIVERS\asyncmac.sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32000  
 Wed Apr 20 02:39:13 2016 Z,mfeaack,McAfee Inc.  
 mfeaack,system32\drivers\mfeaack.sys,Kernel driver,Manual,,@%SystemRoot%\ehome\ehres.dll,-15502  
 Wed Apr 20 02:39:13 2016 Z,mfencbdc,McAfee Inc.  
 mfencbdc,system32\DRIVERS\mfencbdc.sys,Kernel driver,Manual,,McAfee Content driver Copyright (C) 2014 McAfee, Inc. All Rights Reserved.  
 Wed Apr 20 02:37:21 2016 Z,mfefirek,McAfee Inc.  
 mfefirek,system32\drivers\mfefirek.sys,Kernel driver,Manual,,Provides firewall services to McAfee products  
 Wed Apr 20 02:37:20 2016 Z,cfwids,McAfee Inc.  
 cfwids,system32\drivers\cfwids.sys,Kernel driver,Manual,,@%SystemRoot%\System32\certprop.dll,-12  
 Wed Apr 20 02:37:04 2016  
 Z,LanmanServer\Parameters,,%SystemRoot%\system32\svcsvc.dll,,,,,  
 Wed Apr 20 02:37:01 2016 Z,mfemms,McAfee Service Controller,"C:\Program Files\Common Files\McAfee\SystemCore\mfemms.exe",Own\_Process,Auto Start,LocalSystem,Manages McAfee Services  
 Wed Apr 20 02:36:56 2016 Z,vwifimp,Microsoft Virtual WiFi Miniport Service,system32\DRIVERS\vwifimp.sys,Kernel driver,Manual,,Virtual WiFi Filter Driver  
 Wed Apr 20 02:36:49 2016 Z,BrSerIb,Brother Serial Interface Driver(WDM),system32\DRIVERS\BrSerIb.sys,Kernel driver,Manual,,@%systemroot%\system32\browser.dll,-101  
 Wed Apr 20 02:36:49 2016 Z,BrUsbSIb,Brother Serial USB Driver(WDM),system32\DRIVERS\BrUsbSIb.sys,Kernel driver,Manual,,@%systemroot%\system32\browser.dll,-101  
 Wed Apr 20 02:36:49 2016 Z,BthEnum,Bluetooth Enumerator Service,system32\DRIVERS\BthEnum.sys,Kernel driver,Manual,,@%systemroot%\system32\browser.dll,-101  
 Wed Apr 20 02:36:49 2016 Z,BthPan,Bluetooth Device (Personal Area Network),system32\DRIVERS\bthpan.sys,Kernel driver,Manual,,Bluetooth Device (Personal Area Network)  
 Wed Apr 20 02:36:49 2016 Z,monitor,Microsoft Monitor Class Function Driver Service,system32\DRIVERS\monitor.sys,Kernel driver,Manual,,@%systemroot%\system32\mmcsc.dll,-101  
 Wed Apr 20 02:36:49 2016 Z,mouhid,Mouse HID Driver,system32\DRIVERS\mouhid.sys,Kernel driver,Manual,,@%systemroot%\system32\mmcsc.dll,-101  
 Wed Apr 20 02:36:49 2016 Z,RFCOMM,Bluetooth Device (RFCOMM Protocol TDI),system32\DRIVERS\rfcomm.sys,Kernel driver,Manual,,Bluetooth Device (RFCOMM Protocol TDI)  
 Wed Apr 20 02:36:49 2016 Z,usbprint,Microsoft USB PRINTER Class,system32\DRIVERS\usbprint.sys,Kernel driver,Manual,,@%systemroot%\system32\upnpghost.dll,-214  
 Wed Apr 20 02:36:49 2016 Z,usbscan,USB Scanner

## SYSTEM OUTPUT

Driver,system32\DRIVERS\usbscan.sys,Kernel  
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214  
Wed Apr 20 02:36:48 2016 Z,BTHUSB,Bluetooth Radio USB  
Driver,system32\Drivers\BTHUSB.sys,Kernel  
driver,Manual,,@%SystemRoot%\System32\bthserv.dll,-102  
Wed Apr 20 02:36:48 2016 Z,HidUsb,Microsoft HID Class  
Driver,system32\DRIVERS\hidusb.sys,Kernel  
driver,Manual,,@%SystemRoot%\System32\hidserv.dll,-102  
Wed Apr 20 02:36:48 2016 Z,kbdhid,Keyboard HID  
Driver,system32\DRIVERS\kbdhid.sys,Kernel  
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101  
Wed Apr 20 02:36:48 2016  
Z,scfilter,@%SystemRoot%\System32\drivers\scfilter.sys;-11,System32\DRIVERS\scfilter  
.sys,Kernel driver,Manual,,@%SystemRoot%\System32\drivers\scfilter.sys,-12  
Wed Apr 20 02:36:48 2016 Z,WinUSB,WinUSB Service,system32\DRIVERS\WinUSB.sys,Kernel  
driver,Manual,,@%Systemroot%\system32\wsmsvc.dll,-102  
Wed Apr 20 02:36:48 2016 Z,WUDFRd,,system32\DRIVERS\WUDFRd.sys,Kernel  
driver,Manual,,@%systemroot%\system32\wuaueng.dll,-106  
Wed Apr 20 02:36:46 2016 Z,SPUVCbv,SPUVCb Driver  
Service,system32\Drivers\SPUVCbv\_x64.sys,Kernel  
driver,Manual,,@%SystemRoot%\system32\sppuinotify.dll,-102  
Wed Apr 20 02:36:44 2016 Z,usbccgp,Microsoft USB Generic Parent  
Driver,system32\DRIVERS\usbccgp.sys,Kernel  
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214  
Wed Apr 20 02:36:42 2016 Z,mfeavfk,McAfee Inc.  
mfeavfk,system32\drivers\mfeavfk.sys,Kernel  
driver,Manual,,@%SystemRoot%\ehome\ehres.dll,-15502  
Wed Apr 20 02:36:41 2016 Z,AgereSoftModem,Agere Systems Soft  
Modem,system32\DRIVERS\agrsm64.sys,Kernel  
driver,Manual,,@%systemroot%\system32\drivers\afd.sys,-1000  
Wed Apr 20 02:36:41 2016 Z,HdAudAddService,Microsoft 1.1 UAA Function Driver for  
High Definition Audio Service,system32\drivers\HdAudio.sys,Kernel  
driver,Manual,,Keeps your Google software up to date. If this service is disabled or  
stopped, your Google software will not be kept up to date, meaning security  
vulnerabilities that may arise cannot be fixed and features may not work. This  
service uninstalls itself when there is no Google software using it.  
Wed Apr 20 02:36:41 2016 Z,IntcDAud,Intel(R) Display  
Audio,system32\DRIVERS\IntcDAud.sys,Kernel  
driver,Manual,,@%SystemRoot%\system32\ikeext.dll,-502  
Wed Apr 20 02:36:41 2016 Z,ksthunk,Kernel Streaming  
Thunks,\SystemRoot\system32\drivers\ksthunk.sys,Kernel  
driver,Manual,,@keyiso.dll,-101  
Wed Apr 20 02:36:41 2016 Z,Modem,,system32\drivers\modem.sys,Kernel  
driver,Manual,,@%systemroot%\system32\mmcscs.dll,-101  
Wed Apr 20 02:36:41 2016 Z,nusb3hub,Renesas Electronics USB 3.0 Hub  
Driver,\SystemRoot\system32\drivers\nusb3hub.sys,Kernel  
driver,Manual,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1  
Wed Apr 20 02:36:41 2016 Z,Parport,Parallel port

## SYSTEM OUTPUT

```

driver,\SystemRoot\system32\drivers\parport.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\p2psvc.dll,-8007
Wed Apr 20 02:36:41 2016 Z,usbhub,Microsoft USB Standard Hub
Driver,system32\DRIVERS\usbhub.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Wed Apr 20 02:36:38 2016 Z,mssmbios,Microsoft System Management BIOS
Driver,\SystemRoot\system32\drivers\mssmbios.sys,Kernel driver,System Start,,This
service filters e-mail messages on your computer
Wed Apr 20 02:36:34 2016 Z,cdrom,CD-ROM Driver,system32\DRIVERS\cdrom.sys,Kernel
driver,System Start,,ISO9660/Joliet File System Reader for CD/DVDs. (Core) (All
pieces)
Wed Apr 20 02:36:34 2016 Z,Disk,Disk Driver,system32\drivers\disk.sys,Kernel
driver,Boot Start,,@%systemroot%\system32\drivers\discache.sys,-101
Wed Apr 20 02:36:34 2016 Z,hpdskflt,HP Filter,system32\drivers\hpdskflt.sys,Kernel
driver,Boot Start,,McAfee Home Network
Wed Apr 20 02:36:34 2016 Z,rdyboost,ReadyBoost,System32\drivers\rdyboost.sys,Kernel
driver,Boot Start,,ReadyBoost
Wed Apr 20 02:36:33 2016 Z,1394ohci,1394 OHCI Compliant Host
Controller,\SystemRoot\system32\drivers\1394ohci.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\wwansvc.dll,-258
Wed Apr 20 02:36:33 2016 Z,Accelerometer,HP Mobile Data Protection
Sensor,\SystemRoot\system32\drivers\Accelerometer.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\wwansvc.dll,-258
Wed Apr 20 02:36:33 2016 Z,ACPI,Microsoft ACPI
Driver,system32\drivers\ACPI.sys,Kernel driver,Boot
Start,,@%SystemRoot%\System32\wwansvc.dll,-258
Wed Apr 20 02:36:33 2016
Z,AFD,@%systemroot%\system32\drivers\afd.sys;-1000,\SystemRoot\system32\drivers\afd.
sys,Kernel driver,System Start,,@%systemroot%\system32\drivers\afd.sys,-1000
Wed Apr 20 02:36:33 2016 Z,amdkmdag,,system32\DRIVERS\atikmdag.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\Alg.exe,-113
Wed Apr 20 02:36:33 2016 Z,amdkmpfd,AMD PCI Root Bus Lower
Filter,system32\drivers\amdkmpfd.sys,Kernel driver,Boot
Start,,@%SystemRoot%\system32\Alg.exe,-113
Wed Apr 20 02:36:33 2016 Z,atapi,IDE Channel,system32\drivers\atapi.sys,Kernel
driver,Boot Start,,@%systemroot%\system32\rascfg.dll,-32000
Wed Apr 20 02:36:33 2016 Z,Beep,Beep,,Kernel driver,System
Start,,@%SystemRoot%\system32\bdesvc.dll,-101
Wed Apr 20 02:36:33 2016
Z,blbdrive,,\SystemRoot\system32\drivers\blbdrive.sys,Kernel driver,System
Start,,@%SystemRoot%\system32\qmgr.dll,-1001
Wed Apr 20 02:36:33 2016
Z,browser,@%systemroot%\system32\browser.dll;-102,system32\DRIVERS\browser.sys,File
system driver,Manual,,@%systemroot%\system32\browser.dll,-103
Wed Apr 20 02:36:33 2016 Z,cdfs,CD/DVD File System
Reader,system32\DRIVERS\cdfs.sys,File system driver,Disabled,,ISO9660/Joliet File
System Reader for CD/DVDs. (Core) (All pieces)
Wed Apr 20 02:36:33 2016

```

## SYSTEM OUTPUT

Z,CLFS,@%SystemRoot%\system32\clfs.sys;-100,System32\CLFS.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\clfs.sys,-101

Wed Apr 20 02:36:33 2016 Z,CmBatt,Microsoft ACPI Control Method Battery Driver,\SystemRoot\system32\drivers\CmBatt.sys,Kernel driver,Manual,,Microsoft .NET Framework NGEN

Wed Apr 20 02:36:33 2016 Z,CNG,,System32\Drivers\cng.sys,Kernel driver,Boot Start,,Microsoft .NET Framework NGEN

Wed Apr 20 02:36:33 2016 Z,Compbatt,Microsoft Composite Battery Driver,system32\drivers\compbatt.sys,Kernel driver,Boot Start,,Microsoft .NET Framework NGEN

Wed Apr 20 02:36:33 2016 Z,CompositeBus,Composite Bus Enumerator Driver,\SystemRoot\system32\drivers\CompositeBus.sys,Kernel driver,Manual,,Microsoft .NET Framework NGEN

Wed Apr 20 02:36:33 2016

Z,CSC,@%systemroot%\system32\cscsvc.dll;-202,system32\drivers\csc.sys,Kernel driver,System Start,,@%systemroot%\system32\cscsvc.dll,-203

Wed Apr 20 02:36:33 2016

Z,DfsC,@%systemroot%\system32\drivers\dfsc.sys;-101,System32\Drivers\dfsc.sys,File system driver,System Start,,@%systemroot%\system32\drivers\dfsc.sys,-102

Wed Apr 20 02:36:33 2016

Z,discache,@%systemroot%\system32\drivers\discache.sys;-102,System32\drivers\discache.sys,Kernel driver,System Start,,@%systemroot%\system32\drivers\discache.sys,-101

Wed Apr 20 02:36:33 2016 Z,DXGKrnL,LDDM Graphics Subsystem,\SystemRoot\System32\drivers\dxgkrnl.sys,Kernel driver,Manual,,Controls the underlying video driver stacks to provide fully-featured display capabilities.

Wed Apr 20 02:36:33 2016 Z,e1cexpress,Intel(R) PRO/1000 PCI Express Network Connection Driver C,system32\DRIVERS\e1c62x64.sys,Kernel driver,Manual,,Controls the underlying video driver stacks to provide fully-featured display capabilities.

Wed Apr 20 02:36:33 2016 Z,exfat,exFAT File System Driver,,File system driver,Manual,,exFAT File System Driver

Wed Apr 20 02:36:33 2016 Z,fastfat,FAT12/16/32 File System Driver,,File system driver,Manual,,Note - dependance on CDROM.SYS only if required to read/write DVD-RAM media (which appears as CD class device). (Core) (All pieces)

Wed Apr 20 02:36:33 2016

Z,FileInfo,@%SystemRoot%\system32\drivers\fileinfo.sys;-100,system32\drivers\fileinfo.sys,File system driver,Boot Start,,@%SystemRoot%\system32\drivers\fileinfo.sys,-101

Wed Apr 20 02:36:33 2016

Z,FltMgr,@%SystemRoot%\system32\drivers\fltmgr.sys;-10001,system32\drivers\fltmgr.sys,File system driver,Boot Start,,@%SystemRoot%\system32\drivers\fltmgr.sys,-10000

Wed Apr 20 02:36:33 2016 Z,Fs\_Rec,,,8,Boot Start,,@%SystemRoot%\system32\drivers\fsdepends.sys,-10000

Wed Apr 20 02:36:33 2016

Z,fvevol,@%SystemRoot%\system32\drivers\fvevol.sys;-100,System32\DRIVERS\fvevol.sys,Kernel driver;Boot Start,,@%SystemRoot%\system32\drivers\fvevol.sys,-100

Wed Apr 20 02:36:33 2016 Z,HDAudBus,Microsoft UAA Bus Driver for High Definition Audio,\SystemRoot\system32\drivers\HDAudBus.sys,Kernel driver,Manual,,Keeps your Google software up to date. If this service is disabled or stopped, your Google

## SYSTEM OUTPUT

software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Google software using it.

Wed Apr 20 02:36:33 2016

Z,HTTP,\\SystemRoot%\\system32\\drivers\\http.sys;-1,system32\\drivers\\HTTP.sys,Kernel driver,Manual,,\\SystemRoot%\\system32\\drivers\\http.sys,-2

Wed Apr 20 02:36:33 2016

Z,hwpolicy,\\systemroot%\\system32\\drivers\\hwpolicy.sys;-101,system32\\drivers\\hwpolicy.sys,Kernel driver,Boot Start,,\\systemroot%\\system32\\drivers\\hwpolicy.sys,-102

Wed Apr 20 02:36:33 2016 Z,i8042prt,i8042 Keyboard and PS/2 Mouse Port

Driver,\\SystemRoot\\system32\\drivers\\i8042prt.sys,Kernel

driver,Manual,,\\systemroot%\\system32\\drivers\\hwpolicy.sys,-102

Wed Apr 20 02:36:33 2016 Z,igfx,,system32\\DRIVERS\\igdkmd64.sys,Kernel

driver,Manual,,\\SystemRoot%\\system32\\ieetwcollectorres.dll,-1001

Wed Apr 20 02:36:33 2016 Z,intelppm,Intel Processor

Driver,system32\\DRIVERS\\intelppm.sys,Kernel

driver,Manual,,\\SystemRoot%\\system32\\ikeext.dll,-502

Wed Apr 20 02:36:33 2016 Z,JMCR,,system32\\DRIVERS\\jmcr.sys,Kernel

driver,Manual,,\\SystemRoot%\\system32\\drivers\\irenum.sys,-101

Wed Apr 20 02:36:33 2016 Z,kbdclass,Keyboard Class

Driver,system32\\DRIVERS\\kbdclass.sys,Kernel

driver,Manual,,\\SystemRoot%\\system32\\drivers\\irenum.sys,-101

Wed Apr 20 02:36:33 2016 Z,KSecDD,,System32\\Drivers\\ksecdd.sys,Kernel driver,Boot

Start,,@keyiso.dll,-101

Wed Apr 20 02:36:33 2016 Z,KSecPkg,,System32\\Drivers\\ksecpkg.sys,Kernel driver,Boot

Start,,@keyiso.dll,-101

Wed Apr 20 02:36:33 2016 Z,lltdio,Link-Layer Topology Discovery Mapper I/O

Driver,system32\\DRIVERS\\lltdio.sys,Kernel driver,Auto

Start,,\\systemroot%\\system32\\wkssvc.dll,-101

Wed Apr 20 02:36:33 2016

Z,luafv,\\systemroot%\\system32\\drivers\\luafv.sys;-100,\\SystemRoot\\system32\\drivers\\luafv.sys,File system driver,Auto

Start,,\\systemroot%\\system32\\drivers\\luafv.sys,-101

Wed Apr 20 02:36:33 2016

Z,MBAMProtector,,\\??\\C:\\Windows\\system32\\drivers\\mbam.sys,File system

driver,Manual,,\\systemroot%\\system32\\drivers\\luafv.sys,-101

Wed Apr 20 02:36:33 2016

Z,MBAMSwissArmy,MBAMSwissArmy,\\??\\C:\\Windows\\system32\\drivers\\MBAMSwissArmy.sys,File system driver,Manual,,Malwarebytes Anti-Malware service

Wed Apr 20 02:36:33 2016

Z,MBAMWebAccessControl,,\\??\\C:\\Windows\\system32\\drivers\\mwac.sys,File system

driver,Manual,,Malwarebytes Anti-Malware service

Wed Apr 20 02:36:33 2016 Z,MEIx64,Intel(R) Management Engine Interface

,\\SystemRoot\\system32\\drivers\\HECIx64.sys,Kernel

driver,Manual,,\\SystemRoot%\\ehome\\ehres.dll,-15502

Wed Apr 20 02:36:33 2016 Z,mfehidk,McAfee Inc.

mfehidk,system32\\drivers\\mfehidk.sys,Kernel driver,Boot Start,,Provides firewall services to McAfee products

## SYSTEM OUTPUT

Wed Apr 20 02:36:33 2016 Z,mfencrk,McAfee Inc.  
mfencrk,system32\DRIVERS\mfencrk.sys,Kernel driver,Manual,,McAfee Content driver  
Copyright (C) 2014 McAfee, Inc. All Rights Reserved.

Wed Apr 20 02:36:33 2016 Z,mfesapsn,McAfee Process Start Notification  
Service,\\?\C:\Program Files (x86)\McAfee\SiteAdvisor\x64\mfesapsn.sys,Kernel  
driver,Manual,,McAfee Content driver Copyright (C) 2014 McAfee, Inc. All Rights  
Reserved.

Wed Apr 20 02:36:33 2016 Z,mfewfpk,McAfee Inc.  
mfewfpk,system32\drivers\mfewfpk.sys,Kernel driver,Boot Start,,Provides validation  
trust protection services

Wed Apr 20 02:36:33 2016 Z,mouclass,Mouse Class  
Driver,system32\DRIVERS\mouclass.sys,Kernel  
driver,Manual,,@%systemroot%\system32\mmcss.dll,-101

Wed Apr 20 02:36:33 2016  
Z,mountmgr,@%SystemRoot%\system32\drivers\mountmgr.sys;-100,System32\drivers\mountmg  
r.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\mountmgr.sys,-101

Wed Apr 20 02:36:33 2016  
Z,mpsdrv,@%SystemRoot%\system32\FirewallAPI.dll;-23092,System32\drivers\mpsdrv.sys,K  
ernel driver,Manual,,@%SystemRoot%\system32\FirewallAPI.dll,-23093

Wed Apr 20 02:36:33 2016  
Z,mrxsmb,@%systemroot%\system32\wkssvc.dll;-1002,system32\DRIVERS\mrxsmb.sys,File  
system driver,Manual,,@%systemroot%\system32\wkssvc.dll,-1003

Wed Apr 20 02:36:33 2016  
Z,mrxsmb10,@%systemroot%\system32\wkssvc.dll;-1004,system32\DRIVERS\mrxsmb10.sys,File  
system driver,Manual,,@%systemroot%\system32\wkssvc.dll,-1005

Wed Apr 20 02:36:33 2016  
Z,mrxsmb20,@%systemroot%\system32\wkssvc.dll;-1006,system32\DRIVERS\mrxsmb20.sys,File  
system driver,Manual,,@%systemroot%\system32\wkssvc.dll,-1007

Wed Apr 20 02:36:33 2016 Z,msahci,,system32\drivers\msahci.sys,Kernel driver,Boot  
Start,,@%systemroot%\system32\wkssvc.dll,-1007

Wed Apr 20 02:36:33 2016 Z,Msfs,,File system driver,System Start,,@comres.dll,-2798

Wed Apr 20 02:36:33 2016 Z,msisadrv,,system32\drivers\msisadrv.sys,Kernel  
driver,Boot Start,,@%SystemRoot%\system32\drivers\mshidkmdf.sys,-101

Wed Apr 20 02:36:33 2016  
Z,Mup,@%systemroot%\system32\drivers\mup.sys;-101,system32\Drivers\mup.sys,File  
system driver,Boot Start,,@%systemroot%\system32\drivers\mup.sys,-102

Wed Apr 20 02:36:33 2016 Z,NativeWifiP,NativeWiFi  
Filter,system32\DRIVERS\nwifi.sys,Kernel  
driver,Manual,,@%SystemRoot%\system32\qagentrt.dll,-7

Wed Apr 20 02:36:33 2016  
Z,NDIS,@%SystemRoot%\system32\drivers\ndis.sys;-200,system32\drivers\ndis.sys,Kernel  
driver,Boot Start,,@%SystemRoot%\system32\drivers\ndis.sys,-201

Wed Apr 20 02:36:33 2016  
Z,NdisTapi,@%systemroot%\system32\rascfg.dll;-32001,system32\DRIVERS\ndistapi.sys,Ke  
rnel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32001

Wed Apr 20 02:36:33 2016 Z,Ndisuio,NDIS Usermode I/O  
Protocol,system32\DRIVERS\ndisuio.sys,Kernel  
driver,Manual,,@%systemroot%\system32\rascfg.dll,-32001

## SYSTEM OUTPUT

Wed Apr 20 02:36:33 2016  
 Z,NdisWan,@%systemroot%\system32\rascfg.dll;-32002,system32\DRIVERS\ndiswan.sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32002  
 Wed Apr 20 02:36:33 2016 Z,NDProxy,NDIS Proxy,,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32002  
 Wed Apr 20 02:36:33 2016 Z,NetBIOS,NetBIOS Interface,system32\DRIVERS\netbios.sys,File system driver,System Start,,NetBIOS Interface  
 Wed Apr 20 02:36:33 2016  
 Z,NetBT,@%SystemRoot%\system32\drivers\netbt.sys;-2,system32\DRIVERS\netbt.sys,Kernel driver,System Start,,@%SystemRoot%\system32\drivers\netbt.sys,-1  
 Wed Apr 20 02:36:33 2016 Z,NETwNs64,\_\_\_\_ Intel(R) Wireless WiFi Link 5000 Series Adapter Driver for Windows 7 - 64 Bit,system32\DRIVERS\NETwsw00.sys,Kernel driver,Manual,,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallRC.dll,-8200  
 Wed Apr 20 02:36:33 2016 Z,Npfs,,,File system driver,System Start,,@%SystemRoot%\System32\nlasvc.dll,-2  
 Wed Apr 20 02:36:33 2016  
 Z,nsiproxy,@%SystemRoot%\system32\drivers\nsiproxy.sys;-2,system32\drivers\nsiproxy.sys,Kernel driver,System Start,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1  
 Wed Apr 20 02:36:33 2016 Z,Ntfs,,,File system driver,Manual,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1  
 Wed Apr 20 02:36:33 2016 Z,Null,,,Kernel driver,System Start,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1  
 Wed Apr 20 02:36:33 2016 Z,nusb3xhc,Renesas Electronics USB 3.0 Host Controller Driver,\SystemRoot\system32\drivers\nusb3xhc.sys,Kernel driver,Manual,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1  
 Wed Apr 20 02:36:33 2016  
 Z,partmgr,@%SystemRoot%\system32\drivers\partmgr.sys;-100,system32\drivers\partmgr.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\partmgr.sys,-101  
 Wed Apr 20 02:36:33 2016 Z,pci,PCI Bus Driver,system32\drivers\pci.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\pcasvc.dll,-2  
 Wed Apr 20 02:36:33 2016 Z,pcw,Performance Counters for Windows Driver,system32\drivers\pcw.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\pcasvc.dll,-2  
 Wed Apr 20 02:36:33 2016 Z,PEAUTH,PEAUTH,system32\drivers\peauth.sys,Kernel driver,Auto Start,,@%SystemRoot%\system32\pcasvc.dll,-2  
 Wed Apr 20 02:36:33 2016  
 Z,PptpMiniport,@%systemroot%\system32\rascfg.dll;-32006,system32\DRIVERS\raspptp.sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32006  
 Wed Apr 20 02:36:33 2016  
 Z,Psched,@%SystemRoot%\System32\drivers\pacer.sys;-101,system32\DRIVERS\pacer.sys,Kernel driver,System Start,,@%SystemRoot%\System32\drivers\pacer.sys,-101  
 Wed Apr 20 02:36:33 2016 Z,RasAgileVpn,WAN Miniport (IKEv2),system32\DRIVERS\AgileVpn.sys,Kernel driver,Manual,,WAN Miniport (IKEv2)  
 Wed Apr 20 02:36:33 2016  
 Z,Rasl2tp,@%systemroot%\system32\rascfg.dll;-32005,system32\DRIVERS\rasl2tp.sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32005

## SYSTEM OUTPUT

Wed Apr 20 02:36:33 2016  
 Z,RasPppoe,@%systemroot%\system32\rascfg.dll;-32007,system32\DRIVERS\rasppoe.sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32007  
 Wed Apr 20 02:36:33 2016  
 Z,RasSstp,@%systemroot%\system32\sstpsvc.dll;-202,system32\DRIVERS\rassstp.sys,Kernel driver,Manual,,@%systemroot%\system32\sstpsvc.dll,-202  
 Wed Apr 20 02:36:33 2016  
 Z,rdbss,@%systemroot%\system32\wkssvc.dll;-1000,system32\DRIVERS\rdbss.sys,File system driver,System Start,,@%systemroot%\system32\wkssvc.dll,-1001  
 Wed Apr 20 02:36:33 2016 Z,rdpbus,Remote Desktop Device Redirector Bus Driver,\SystemRoot\system32\drivers\rdpbus.sys,Kernel driver,Manual,,@%systemroot%\system32\wkssvc.dll,-1001  
 Wed Apr 20 02:36:33 2016  
 Z,RDPCDD,@%systemroot%\system32\DRIVERS\RDPCDD.sys;-100,system32\DRIVERS\RDPCDD.sys,Kernel driver,System Start,,@%systemroot%\system32\DRIVERS\RDPCDD.sys,-101  
 Wed Apr 20 02:36:33 2016  
 Z,RDPENCDD,@%systemroot%\system32\drivers\RDPCDD.sys;-101,system32\drivers\rdpencd.sys,Kernel driver,System Start,,@%systemroot%\system32\drivers\RDPCDD.sys,-100  
 Wed Apr 20 02:36:33 2016  
 Z,RDPREFMP,@%systemroot%\system32\drivers\RdpRefMp.sys;-101,system32\drivers\rdprefmp.sys,Kernel driver,System Start,,@%systemroot%\system32\drivers\RdpRefMp.sys,-100  
 Wed Apr 20 02:36:33 2016 Z,rsnpsdr,Link-Layer Topology Discovery Responder,system32\DRIVERS\rsnpsdr.sys,Kernel driver,Auto Start,,@oleres.dll,-5011  
 Wed Apr 20 02:36:33 2016 Z,secdrv,Security Driver,,Kernel driver,Disabled,,@%SystemRoot%\system32\sdrrvc.dll,-102  
 Wed Apr 20 02:36:33 2016 Z,Serenum,Serenum Filter Driver,system32\DRIVERS\serenum.sys,Kernel driver,Manual,,@%SystemRoot%\System32\sensrvc.dll,-1001  
 Wed Apr 20 02:36:33 2016 Z,Serial,Serial port driver,system32\DRIVERS\serial.sys,Kernel driver,System Start,,@%SystemRoot%\System32\sensrvc.dll,-1001  
 Wed Apr 20 02:36:33 2016 Z,spldr,Security Processor Loader Driver,,Kernel driver,Boot Start,,@%SystemRoot%\system32\snmptrap.exe,-4  
 Wed Apr 20 02:36:33 2016  
 Z,srv,@%systemroot%\system32\srvc.dll;-102,system32\DRIVERS\srvc.sys,File system driver,Manual,,@%systemroot%\system32\srvc.dll,-103  
 Wed Apr 20 02:36:33 2016  
 Z,srv2,@%systemroot%\system32\srvc.dll;-104,system32\DRIVERS\srvc2.sys,File system driver,Manual,,@%systemroot%\system32\srvc.dll,-105  
 Wed Apr 20 02:36:33 2016 Z,srvnet,,system32\DRIVERS\srvcnet.sys,File system driver,Manual,,@%systemroot%\system32\srvc.dll,-105  
 Wed Apr 20 02:36:33 2016  
 Z,storflt,@%SystemRoot%\system32\vmstorfltres.dll;-1000,system32\drivers\vmstorflt.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\wiaservc.dll,-10  
 Wed Apr 20 02:36:33 2016 Z,swenum,Software Bus Driver,\SystemRoot\system32\drivers\swenum.sys,Kernel driver,Manual,,@%SystemRoot%\System32\StorSvc.dll,-101  
 Wed Apr 20 02:36:33 2016



## SYSTEM OUTPUT

Z,Tcpip,@%SystemRoot%\system32\tcpipcfg.dll;-50003,System32\drivers\tcpip.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\tcpipcfg.dll,-50003

Wed Apr 20 02:36:33 2016 Z,tcpipreg,TCP/IP Registry Compatibility,System32\drivers\tcpipreg.sys,Kernel driver,Auto Start,,Provides compatibility for legacy applications which interact with TCP/IP through the registry. If this service is stopped, certain applications may have impaired functionality.

Wed Apr 20 02:36:33 2016 Z,tdx,@%SystemRoot%\system32\tcpipcfg.dll;-50004,system32\DRIVERS\tdx.sys,Kernel driver,System Start,,@%SystemRoot%\system32\tcpipcfg.dll,-50004

Wed Apr 20 02:36:33 2016 Z,TermDD,Terminal Device Driver,\SystemRoot\system32\drivers\termdd.sys,Kernel driver,System Start,,@%SystemRoot%\system32\tcpipcfg.dll,-50004

Wed Apr 20 02:36:33 2016 Z,TPM,TPM,system32\drivers\tpm.sys,Kernel driver,Manual,,TPM Driver

Wed Apr 20 02:36:33 2016 Z,tunnel,Microsoft Tunnel Miniport Adapter Driver,system32\DRIVERS\tunnel.sys,Kernel driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000

Wed Apr 20 02:36:33 2016 Z,udfs,udfs,system32\DRIVERS\udfs.sys,File system driver,Disabled,,Reads/Writes UDF 1.02,1.5,2.0x,2.5 disc formats, usually found on C/DVD discs. (Core) (All pieces)

Wed Apr 20 02:36:33 2016 Z,umbus,UMBus Enumerator Driver,\SystemRoot\system32\drivers\umbus.sys,Kernel driver,Manual,,@%SystemRoot%\system32\ui0detect.exe,-102

Wed Apr 20 02:36:33 2016 Z,usbehci,Microsoft USB 2.0 Enhanced Host Controller Miniport Driver,\SystemRoot\system32\drivers\usbehci.sys,Kernel driver,Manual,,@%systemroot%\system32\upnphost.dll,-214

Wed Apr 20 02:36:33 2016 Z,vdrvroot,Microsoft Virtual Drive Enumerator Driver,system32\drivers\vdrvroot.sys,Kernel driver,Boot Start,,Validity Fingerprint Service

Wed Apr 20 02:36:33 2016 Z,VgaSave,,\SystemRoot\System32\drivers\vga.sys,Kernel driver,System Start,,@%SystemRoot%\system32\vds.exe,-112

Wed Apr 20 02:36:33 2016 Z,volmgr,Volume Manager Driver,system32\drivers\volmgr.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\vds.exe,-112

Wed Apr 20 02:36:33 2016 Z,volmgrx,@%SystemRoot%\system32\drivers\volmgrx.sys;-100,system32\drivers\volmgrx.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\volmgrx.sys,-101

Wed Apr 20 02:36:33 2016 Z,volsnap,Storage volumes,system32\drivers\volsnap.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\volmgrx.sys,-101

Wed Apr 20 02:36:33 2016 Z,vwifibus,Virtual WiFi Bus Driver,system32\DRIVERS\vwifibus.sys,Kernel driver,Manual,,Virtual WiFi Bus Driver

Wed Apr 20 02:36:33 2016 Z,vwififlt,Virtual WiFi Filter Driver,system32\DRIVERS\vwififlt.sys,Kernel driver,System Start,,Virtual WiFi Filter Driver

Wed Apr 20 02:36:33 2016 Z,Wanarpv6,@%systemroot%\system32\rascfg.dll;-32012,system32\DRIVERS\wanarp.sys,Kern

## SYSTEM OUTPUT

```

el driver,System Start,,@%systemroot%\system32\rascfg.dll,-32012
Wed Apr 20 02:36:33 2016
Z,Wdf01000,@%SystemRoot%\system32\drivers\Wdf01000.sys;-1000,system32\drivers\Wdf01000.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\WcsPlugInService.dll,-201
Wed Apr 20 02:36:33 2016 Z,WfpLwf,WFP Lightweight Filter,system32\DRIVERS\wfpLwf.sys,Kernel driver,System Start,,WFP Lightweight Filter
Wed Apr 20 02:36:33 2016 Z,WIMMount,WIMMount,system32\drivers\wimmount.sys,File system driver,Manual,,WIM Image mount service driver
Wed Apr 20 02:36:33 2016 Z,WmiAcpi,Microsoft Windows Management Interface for ACPI,\SystemRoot\system32\drivers\wmiaapi.sys,Kernel driver,Manual,,@%SystemRoot%\System32\wlansvc.dll,-258
Wed Apr 20 02:36:33 2016 Z,ws2ifsl,Windows Socket 2.0 Non-IFS Service Provider Support Environment,\SystemRoot\system32\drivers\ws2ifsl.sys,Kernel driver,System Start,,@%systemroot%\System32\drivers\ws2ifsl.sys,-1000
Wed Apr 20 02:36:33 2016
Z,WudfPff,@%SystemRoot%\system32\drivers\WudfPff.sys;-1000,system32\drivers\WudfPff.sys,Kernel driver,Manual,,@%systemroot%\system32\wuaueng.dll,-106
Tue Apr 19 01:25:12 2016 Z,MSK80Service,McAfee Anti-Spam Service,"C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,Share_Process,Auto Start,LocalSystem,This service filters e-mail messages on your computer
Tue Apr 19 01:25:10 2016 Z,McProxy,McAfee Proxy Service,"C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,Share_Process,Auto Start,LocalSystem,McAfee Proxy Service
Tue Apr 19 01:25:09 2016 Z,McNaiAnn,McAfee VirusScan Announcer,"C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,Share_Process,Auto Start,LocalSystem,McAfee VirusScan Announcer
Tue Apr 19 01:25:08 2016 Z,McMPFSvc,McAfee Personal Firewall Service,"C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,Share_Process,Auto Start,LocalSystem,Helps protect your computer from intrusion and let's you manage your computer's trusted programs.
Tue Apr 19 01:25:06 2016 Z,McBootDelayStartSvc,McAfee Boot Delay Start Service,"C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,Share_Process,Auto Start,LocalSystem,McAfee Boot Delay Start Service
Tue Apr 19 01:25:05 2016 Z,HomeNetSvc,McAfee Home Network,"C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,Share_Process,Auto Start,LocalSystem,McAfee Home Network
Tue Apr 19 01:25:04 2016 Z,McAPExe,McAfee AP Service,"C:\Program Files\McAfee\MSM\McAPExe.exe",Own_Process,Auto Start,LocalSystem,McAfee AP Service
Tue Apr 19 01:25:03 2016 Z,mfefire,McAfee Firewall Core Service,"C:\Program Files\Common Files\McAfee\SystemCore\mfefire.exe",Own_Process,Manual,LocalSystem,Provides firewall services to McAfee products
Tue Apr 19 01:25:00 2016 Z,mfevtp,McAfee Validation Trust Protection Service,"C:\Windows\system32\mfevtps.exe",Own_Process,Manual,LocalSystem,Provides validation trust protection services
Tue Apr 19 01:22:11 2016 Z,McAfee SiteAdvisor Service,McAfee SiteAdvisor

```

## SYSTEM OUTPUT

Service,"C:\Program Files (x86)\McAfee\SiteAdvisor\McSACore.exe",Own\_Process,Auto Start,LocalSystem,McAfee SiteAdvisor Service  
 Tue Apr 19 01:21:52 2016 Z,mcpltsvc,McAfee Platform Services,"C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvcHost.exe"  
 /McCoreSvc,Share\_Process,Auto Start,LocalSystem,McAfee Platform Services  
 Tue Apr 19 01:21:37 2016 Z,PEFService,Intel Security PEF Service,"C:\Program Files\Common Files\Intel Security\PEF\CORE\PEFService.exe",Own\_Process,Auto Start,LocalSystem,Intel Security PEF Service  
 Tue Apr 19 01:21:20 2016 Z,mccspsvc,McAfee CSP Service,"C:\Program Files\Common Files\McAfee\CSP\1.8.267.0\McCSPServiceHost.exe",Own\_Process,Auto Start,LocalSystem,McAfee Cloud Platform Service  
 Sat Apr 16 22:47:57 2016 Z,MSPQM,Microsoft Streaming Quality Manager Proxy,system32\drivers\MSPQM.sys,Kernel driver,Manual,,This service filters e-mail messages on your computer  
 Wed Apr 13 11:43:26 2016  
 Z,TrustedInstaller,@%SystemRoot%\servicing\TrustedInstaller.exe;-100,%SystemRoot%\servicing\TrustedInstaller.exe,Own\_Process,Manual,localSystem,@%SystemRoot%\servicing\TrustedInstaller.exe;-101  
 Wed Apr 13 11:42:56 2016  
 Z,PlugPlay\Parameters,,%SystemRoot%\system32\umpnpmgr.dll,,,  
 Wed Apr 6 14:20:46 2016 Z,USBSTOR,USB Mass Storage Driver,system32\DRIVERS\USBSTOR.SYS,Kernel driver,Manual,,@%systemroot%\system32\upnphost.dll,-214  
 Wed Apr 6 00:30:11 2016  
 Z,Winmgmt\Parameters,,%SystemRoot%\system32\wbem\WMISvc.dll,,,  
 Sun Mar 27 00:31:42 2016 Z,MBAMSchedular,"C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamschedular.exe",Own\_Process,Auto Start,LocalSystem,Malwarebytes Anti-Malware scheduler  
 Sun Mar 27 00:31:41 2016 Z,MBAMService,"C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamservice.exe",Own\_Process,Auto Start,LocalSystem,Malwarebytes Anti-Malware service  
 Thu Mar 10 19:38:21 2016 Z,Netaapl,Apple Mobile Device Ethernet Service,system32\DRIVERS\netaapl64.sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32002  
 Thu Mar 10 19:38:21 2016 Z,USBAAPL64,Apple Mobile USB Driver,System32\Drivers\usbaapl64.sys,Kernel driver,Manual,,@%systemroot%\system32\upnphost.dll,-214  
 Thu Feb 25 02:16:29 2016 Z,usbaudio,USB Audio Driver (WDM),system32\drivers\usbaudio.sys,Kernel driver,Manual,,@%systemroot%\system32\upnphost.dll,-214  
 Sun Feb 21 00:01:18 2016 Z,WinDefend,@%ProgramFiles%\Windows Defender\MsMpRes.dll;-103,%SystemRoot%\System32\svchost.exe -k secsvcs,Share\_Process,Manual,LocalSystem,@%ProgramFiles%\Windows Defender\MsMpRes.dll,-1176  
 Sun Feb 14 15:57:33 2016 Z,drmkaud,Microsoft Trusted Audio Drivers,\SystemRoot\system32\drivers\drmkaud.sys,Kernel driver,Manual,,@%systemroot%\system32\dps.dll,-501  
 Sun Feb 14 15:57:33 2016 Z,MSKSSRV,Microsoft Streaming Service

## SYSTEM OUTPUT

Proxy,system32\drivers\MSKSSRV.sys,Kernel driver,Manual,,This service filters e-mail messages on your computer  
 Sun Feb 14 15:57:33 2016 Z,MSPCLOCK,Microsoft Streaming Clock  
 Proxy,system32\drivers\MSPCLOCK.sys,Kernel driver,Manual,,This service filters e-mail messages on your computer  
 Sun Feb 14 15:57:33 2016 Z,MSTEE,Microsoft Streaming Tee/Sink-to-Sink Converter,system32\drivers\MSTEE.sys,Kernel driver,Manual,,This service filters e-mail messages on your computer  
 Wed Feb 10 01:34:39 2016 Z,tap0901,TAP-Windows Adapter V9,system32\DRIVERS\tap0901.sys,Kernel driver,Manual,,@%SystemRoot%\system32\TabSvc.dll,-101  
 Tue Feb 9 22:07:39 2016 Z,clr\_optimization\_v2.0.50727\_32,Microsoft .NET Framework NGEN  
 v2.0.50727\_X86,%systemroot%\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe,Own\_Process,Disabled,LocalSystem,Microsoft .NET Framework NGEN  
 Tue Feb 9 22:07:39 2016 Z,clr\_optimization\_v2.0.50727\_64,Microsoft .NET Framework NGEN  
 v2.0.50727\_X64,%systemroot%\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe,Own\_Process,Disabled,LocalSystem,Microsoft .NET Framework NGEN  
 Wed Feb 3 04:32:57 2016  
 Z,BITS,@%SystemRoot%\system32\qmgr.dll;-1000,%SystemRoot%\System32\svchost.exe -k netsvcs,Share\_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\qmgr.dll,-1001  
 Tue Feb 2 00:31:05 2016 Z,BrYNSvc,BrYNSvc,"C:\Program Files (x86)\Browny02\BrYNSvc.exe",Own\_Process,Manual,LocalSystem,@%systemroot%\system32\browser.dll,-101  
 Tue Feb 2 00:20:01 2016 Z,PDFProFiltSrvPP,PDFProFiltSrvPP,C:\Program Files (x86)\Nuance\PaperPort\PDFProFiltSrvPP.exe,Own\_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\pcasvc.dll,-2  
 Mon Feb 1 03:04:18 2016 Z,StillCam,Still Serial Digital Camera Driver,system32\DRIVERS\serscan.sys,Kernel driver,Manual,,@%SystemRoot%\system32\sstpsvc.dll,-201  
 Tue Jan 19 22:34:35 2016 Z,IntuitUpdateServiceV4,Intuit Update Service v4,"C:\Program Files (x86)\Common Files\Intuit\Update Service v4\IntuitUpdateService.exe",Own\_Process,Auto Start,LocalSystem,Helps Intuit applications automatically update themselves.  
 Tue Jan 19 22:14:22 2016  
 Z,msiserver,@%SystemRoot%\system32\msimsg.dll;-27,%systemroot%\system32\msiexec.exe /V,Own\_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\msimsg.dll,-32  
 Thu Jan 7 22:15:30 2016 Z,iPod Service,iPod Service,"C:\Program Files\iPod\bin\iPodService.exe",Own\_Process,Manual,LocalSystem,iPod hardware management services  
 Thu Jan 7 22:11:07 2016 Z,Bonjour Service,Bonjour Service,"C:\Program Files\Bonjour\mDNSResponder.exe",Own\_Process,Auto Start,LocalSystem,Enables hardware devices and software services to automatically configure themselves on the network and advertise their presence.  
 Fri Jan 1 20:52:19 2016 Z,MozillaMaintenance,Mozilla Maintenance Service,"C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe",Own\_Process,Manual,LocalSystem,The Mozilla

## SYSTEM OUTPUT

Maintenance Service ensures that you have the latest and most secure version of Mozilla Firefox on your computer. Keeping Firefox up to date is very important for your online security, and Mozilla strongly recommends that you keep this service enabled.

Sat Nov 28 20:21:16 2015

Z,{1BDD94C3-9D85-46F0-87E3-BD3288A5F6BD},,,,,,@%SystemRoot%\System32\wwansvc.dll,-258

Wed Nov 11 20:32:01 2015

Z,SharedAccess\Parameters,,%SystemRoot%\System32\ipnathlp.dll,,,,

Wed Nov 11 20:31:53 2015

Z,SharedAccess,@%SystemRoot%\system32\ipnathlp.dll;-106,%SystemRoot%\System32\svchost.exe -k

netshvcs,Share\_Process,Manual,LocalSystem,@%SystemRoot%\system32\ipnathlp.dll,-107

Wed Nov 11 20:31:50 2015

Z,{A9E50A43-973B-4CAD-B78E-EA0321A4A293},,,,,,@%SystemRoot%\System32\wwansvc.dll,-258

Mon Oct 19 23:21:21 2015 Z,MSDTC Bridge 4.0.0.0,,,,,@comres.dll,-2798

Mon Oct 19 23:21:21 2015 Z,SMSvcHost

4.0.0.0,,,,,@%SystemRoot%\system32\tcpipcfg.dll,-50006

Mon Oct 19 23:21:21 2015 Z,Windows Workflow Foundation

4.0.0.0,,,,,@ProgramFiles%\Windows Defender\MsMpRes.dll,-1176

Fri Oct 2 14:28:51 2015 Z,McODS,McAfee Scanner,"C:\Program

Files\McAfee\VirusScan\mcods.exe",Own\_Process,Manual,LocalSystem,McAfee Scanner

Wed Sep 23 03:20:38 2015 Z,usbvideo,USB Video Device

(WDM),System32\Drivers\usbvideo.sys,Kernel

driver,Manual,,@%systemroot%\system32\upnphost.dll,-214

Sat Sep 12 00:14:59 2015 Z,ASP.NET,,,,,@appmgmts.dll,-3251

Sat Sep 12 00:14:57 2015 Z,ASP.NET\_4.0.30319,,,,,@appmgmts.dll,-3251

Sat Sep 12 00:14:57 2015 Z,aspnet\_state,ASP.NET State

Service,%SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\aspnet\_state.exe,Own\_Process,Disabled,NT AUTHORITY\NetworkService,Provides support for out-of-process session states for ASP.NET. If this service is stopped, out-of-process requests will not be processed. If this service is disabled, any services that explicitly depend on it will fail to start.

Sat Sep 12 00:14:30 2015

Z,NetMsmqActivator,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallRC.dll;-8195,"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe"

-NetMsmqActivator,Share\_Process,Disabled,NT

AUTHORITY\NetworkService,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallRC.dll,-8194

Sat Sep 12 00:14:29 2015

Z,NetPipeActivator,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallRC.dll;-8197,C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe,Share

\_Process,Disabled,NT

AUTHORITY\LocalService,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallRC.dll,-8196

Sat Sep 12 00:14:25 2015

Z,NetTcpActivator,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInst

## SYSTEM OUTPUT

allRC.dll;-8199,C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSSvcHost.exe,Share\_Process,Disabled,NT  
 AUTHORITY\LocalService,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallRC.dll,-8198  
 Sat Sep 12 00:14:23 2015  
 Z,NetTcpPortSharing,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallRC.dll;-8201,C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSSvcHost.exe,Share\_Process,Disabled,NT  
 AUTHORITY\LocalService,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallRC.dll,-8200  
 Sat Sep 12 00:14:19 2015 Z,.NET Memory Cache  
 4.0,,,,,@%SystemRoot%\System32\wwansvc.dll,-258  
 Sat Sep 12 00:09:28 2015  
 Z,stisvc,@%SystemRoot%\system32\wiaservc.dll;-9,%SystemRoot%\system32\svchost.exe -k
 Authority\LocalService,@%SystemRoot%\system32\wiaservc.dll,-10  
 Fri Sep 11 18:30:16 2015 Z,Apple Mobile Device,,,,,@%systemroot%\system32\appinfo.dll,-101  
 Fri Sep 11 17:57:59 2015 Z,Apple Mobile Device Service,Apple Mobile Device Service,"C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe",Own\_Process,Auto Start,LocalSystem,Provides the interface to Apple mobile devices.  
 Fri Sep 11 14:56:27 2015 Z,gupdate,Google Update Service (gupdate),"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /svc,Own\_Process,Auto Start,LocalSystem,Keeps your Google software up to date. If this service is disabled or stopped, your Google software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Google software using it.  
 Fri Sep 11 14:56:27 2015 Z,gupdatem,Google Update Service (gupdatem),"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /medsvc,Own\_Process,Manual,LocalSystem,Keeps your Google software up to date. If this service is disabled or stopped, your Google software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Google software using it.  
 Fri Sep 11 07:47:27 2015  
 Z,WbioSrv,@%systemroot%\system32\wbiosrv.dll;-100,%SystemRoot%\system32\svchost.exe -k  
 WbioSvcGroup,Share\_Process,Manual,LocalSystem,@%systemroot%\system32\wbiosrv.dll,-101  
 Thu Sep 10 21:49:02 2015 Z,clr\_optimization\_v4.0.30319\_64,Microsoft .NET Framework NGEN  
 v4.0.30319\_X64,C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe,Own\_Process,Auto Start,LocalSystem,Microsoft .NET Framework NGEN  
 Thu Sep 10 21:49:01 2015 Z,clr\_optimization\_v4.0.30319\_32,Microsoft .NET Framework NGEN  
 v4.0.30319\_X86,C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe,Own\_Process,Auto Start,LocalSystem,Microsoft .NET Framework NGEN

## SYSTEM OUTPUT

Thu Sep 10 21:48:06 2015 Z,.NET CLR Networking  
 4.0.0.0,,,,,@%SystemRoot%\System32\wwansvc.dll,-258  
 Thu Sep 10 21:30:14 2015  
 Z,eventlog,@%SystemRoot%\system32\wevtstvc.dll;-200,%SystemRoot%\System32\svchost.exe  
 -k LocalServiceNetworkRestricted,Share\_Process,Auto Start,NT  
 AUTHORITY\LocalService,@%SystemRoot%\system32\wevtstvc.dll,-201  
 Thu Sep 10 21:30:14 2015 Z,Outlook,,,,,Office Software Protection Platform Service  
 (unlocalized description)  
 Thu Sep 10 21:28:37 2015 Z,osppsvc,Office Software Protection Platform,"C:\Program  
 Files\Common Files\Microsoft  
 Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE",Own\_Process,Manual,NT  
 AUTHORITY\NetworkService,Office Software Protection Platform Service (unlocalized  
 description)  
 Thu Sep 10 20:46:43 2015  
 Z,DiagTrack,@%SystemRoot%\system32\UtcResources.dll;-3001,%SystemRoot%\System32\svch  
 ost.exe -k utcsvc,Own\_Process,Auto  
 Start,LocalSystem,@%SystemRoot%\system32\UtcResources.dll,-3002  
 Thu Sep 10 20:46:43 2015  
 Z,DiagTrack\Parameters,,%SystemRoot%\system32\diagtrack.dll,,,  
 Thu Sep 10 19:42:05 2015 Z,ose,Office Source Engine,"C:\Program Files (x86)\Common  
 Files\Microsoft Shared\Source Engine\OSE.EXE",Own\_Process,Manual,LocalSystem,Saves  
 installation files used for updates and repairs and is required for the downloading  
 of Setup updates and Watson error reports.  
 Thu Sep 10 17:10:15 2015  
 Z,IKEEXT,@%SystemRoot%\system32\ikeext.dll;-501,%systemroot%\system32\svchost.exe -k  
 netsvcs,Share\_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\ikeext.dll,-502  
 Thu Sep 10 17:09:34 2015 Z,HipShieldK,McAfee Inc.  
 HipShieldK,system32\drivers\HipShieldK.sys,Kernel  
 driver,Manual,,@%SystemRoot%\System32\hidserv.dll,-102  
 Thu Sep 10 16:33:32 2015 Z,odserv,Microsoft Office Diagnostics Service,"C:\Program  
 Files (x86)\Common Files\Microsoft  
 Shared\OFFICE12\ODSERV.EXE",Own\_Process,Manual,LocalSystem,Run portions of Microsoft  
 Office Diagnostics.  
 Thu Sep 10 04:09:03 2015 Z,WMPNetworkSvc,@%PROGRAMFILES%\Windows Media  
 Player\wmpnetwk.exe;-101,"%PROGRAMFILES%\Windows Media  
 Player\wmpnetwk.exe",Own\_Process,Auto Start,NT  
 AUTHORITY\NetworkService,@%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-102  
 Thu Sep 10 04:09:02 2015  
 Z,HomeGroupListener,@%SystemRoot%\System32\ListSvc.dll;-100,%SystemRoot%\System32\sv  
 chost.exe -k  
 LocalSystemNetworkRestricted,Share\_Process,Manual,LocalSystem,@%SystemRoot%\System32  
 \ListSvc.dll,-101  
 Thu Sep 10 04:08:46 2015  
 Z,FDResPub,@%systemroot%\system32\fdrespub.dll;-100,%SystemRoot%\system32\svchost.ex  
 e -k LocalServiceAndNoImpersonation,Share\_Process,Auto Start,NT  
 AUTHORITY\LocalService,@%systemroot%\system32\fdrespub.dll,-101  
 Thu Sep 3 18:12:30 2015  
 Z,WSearch,@%systemroot%\system32\SearchIndexer.exe;-103,%systemroot%\system32\Search

## SYSTEM OUTPUT

```

Indexer.exe /Embedding,Own_Process,Auto
Start,LocalSystem,@%systemroot%\system32\SearchIndexer.exe,-104
Thu Sep  3 17:49:58 2015
Z,CertPropSvc,@%SystemRoot%\System32\certprop.dll;-11,%SystemRoot%\system32\svchost.
exe -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\System32\certprop.dll,-12
Thu Sep  3 17:49:58 2015
Z,SCardSvr,@%SystemRoot%\System32\SCardSvr.dll;-1,%SystemRoot%\system32\svchost.exe
-k LocalServiceAndNoImpersonation,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\SCardSvr.dll,-5
Thu Sep  3 17:49:37 2015
Z,{720B974A-3E6B-42BF-9839-4EE6CD676477},,,,,,%SystemRoot%\System32\wwansvc.dll,-25
8
Fri Feb 20 18:42:20 2015 Z,adp94xx,,\SystemRoot\system32\drivers\adp94xx.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\wwansvc.dll,-258
Fri Feb 20 18:42:20 2015 Z,adpahci,,\SystemRoot\system32\drivers\adpahci.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\wwansvc.dll,-258
Fri Feb 20 18:42:20 2015 Z,adpu320,,\SystemRoot\system32\drivers\adpu320.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\wwansvc.dll,-258
Fri Feb 20 18:42:20 2015 Z,aliide,,\SystemRoot\system32\drivers\aliide.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\Alg.exe,-113
Fri Feb 20 18:42:20 2015 Z,amdide,,\SystemRoot\system32\drivers\amdide.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\Alg.exe,-113
Fri Feb 20 18:42:20 2015 Z,amdsata,,\SystemRoot\system32\drivers\amdsata.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\Alg.exe,-113
Fri Feb 20 18:42:20 2015 Z,amdsbs,,\SystemRoot\system32\drivers\amdsbs.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\Alg.exe,-113
Fri Feb 20 18:42:20 2015 Z,arc,,\SystemRoot\system32\drivers\arc.sys,Kernel
driver,Manual,,@appmgmts.dll,-3251
Fri Feb 20 18:42:20 2015 Z,arcsas,,\SystemRoot\system32\drivers\arcsas.sys,Kernel
driver,Manual,,@appmgmts.dll,-3251
Fri Feb 20 18:42:20 2015 Z,cmdide,,\SystemRoot\system32\drivers\cmdide.sys,Kernel
driver,Manual,,Microsoft .NET Framework NGEN
Fri Feb 20 18:42:20 2015 Z,elxstor,,\SystemRoot\system32\drivers\elxstor.sys,Kernel
driver,Manual,,@%SystemRoot%\ehome\ehsched.exe,-102
Fri Feb 20 18:42:20 2015 Z,HpSAMD,,\SystemRoot\system32\drivers\HpSAMD.sys,Kernel
driver,Manual,,McAfee Home Network
Fri Feb 20 18:42:20 2015 Z,iaStorV,,\SystemRoot\system32\drivers\iaStorV.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
Fri Feb 20 18:42:20 2015 Z,iirsp,,\SystemRoot\system32\drivers\iirsp.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ieetwcollectorres.dll,-1001
Fri Feb 20 18:42:20 2015
Z,intelide,,\SystemRoot\system32\drivers\intelide.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ikeext.dll,-502
Fri Feb 20 18:42:20 2015 Z,isapnp,,\SystemRoot\system32\drivers\isapnp.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Fri Feb 20 18:42:20 2015 Z,LSI_FC,,\SystemRoot\system32\drivers\lsi_fc.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\lmhsvc.dll,-102

```



## SYSTEM OUTPUT

```

Fri Feb 20 18:42:20 2015 Z,LSI_SAS,,\SystemRoot\system32\drivers\lsi_sas.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\lmhsvc.dll,-102
Fri Feb 20 18:42:20 2015
Z,LSI_SAS2,,\SystemRoot\system32\drivers\lsi_sas2.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\lmhsvc.dll,-102
Fri Feb 20 18:42:20 2015
Z,LSI_SCSI,,\SystemRoot\system32\drivers\lsi_scsi.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\lmhsvc.dll,-102
Fri Feb 20 18:42:20 2015 Z,megasas,,\SystemRoot\system32\drivers\megasas.sys,Kernel
driver,Manual,,@%SystemRoot%\ehome\ehres.dll,-15502
Fri Feb 20 18:42:20 2015 Z,MegaSR,,\SystemRoot\system32\drivers\MegaSR.sys,Kernel
driver,Manual,,@%SystemRoot%\ehome\ehres.dll,-15502
Fri Feb 20 18:42:20 2015 Z,mpio,,\SystemRoot\system32\drivers\mpio.sys,Kernel
driver,Manual,,The Mozilla Maintenance Service ensures that you have the latest and
most secure version of Mozilla Firefox on your computer. Keeping Firefox up to date
is very important for your online security, and Mozilla strongly recommends that you
keep this service enabled.
Fri Feb 20 18:42:20 2015 Z,msdsm,,\SystemRoot\system32\drivers\msdsm.sys,Kernel
driver,Manual,,@%systemroot%\system32\wkssvc.dll,-1007
Fri Feb 20 18:42:20 2015 Z,nfrd960,,\SystemRoot\system32\drivers\nfrd960.sys,Kernel
driver,Manual,,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstall
RC.dll,-8200
Fri Feb 20 18:42:20 2015 Z,nvraid,,\SystemRoot\system32\drivers\nvraid.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Fri Feb 20 18:42:20 2015 Z,nvstor,,\SystemRoot\system32\drivers\nvstor.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Fri Feb 20 18:42:20 2015 Z,pciide,,\SystemRoot\system32\drivers\pciide.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\pcasvc.dll,-2
Fri Feb 20 18:42:20 2015 Z,ql2300,,\SystemRoot\system32\drivers\ql2300.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\drivers\pacer.sys,-101
Fri Feb 20 18:42:20 2015 Z,ql40xx,,\SystemRoot\system32\drivers\ql40xx.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\drivers\pacer.sys,-101
Fri Feb 20 18:42:20 2015
Z,sbp2port,,\SystemRoot\system32\drivers\sbp2port.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\samsrv.dll,-2
Fri Feb 20 18:42:20 2015
Z,SiSRaid2,,\SystemRoot\system32\drivers\SiSRaid2.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\shsvcs.dll,-12289
Fri Feb 20 18:42:20 2015
Z,SiSRaid4,,\SystemRoot\system32\drivers\sisraid4.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\shsvcs.dll,-12289
Fri Feb 20 18:42:20 2015
Z,stexstor,,\SystemRoot\system32\drivers\stexstor.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\sstpsvc.dll,-201
Fri Feb 20 18:42:20 2015 Z,storvsc,,\SystemRoot\system32\drivers\storvsc.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\StorSvc.dll,-101
Fri Feb 20 18:42:20 2015 Z,viaide,,\SystemRoot\system32\drivers\viaide.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\vds.exe,-112

```

## SYSTEM OUTPUT

Fri Feb 20 18:42:20 2015 Z,vmbus,,\SystemRoot\system32\drivers\vmbus.sys,Kernel  
 driver,Manual,,@%SystemRoot%\system32\vs.exe,-112  
 Fri Feb 20 18:42:20 2015 Z,vsmraid,,\SystemRoot\system32\drivers\vsmraid.sys,Kernel  
 driver,Manual,,@%SystemRoot%\system32\drivers\volmgrx.sys,-101  
 Fri Feb 20 18:42:20 2015 Z,Wd,,\SystemRoot\system32\drivers\wd.sys,Kernel  
 driver,Manual,,@%SystemRoot%\system32\WcsPlugInService.dll,-201  
 Fri Feb 20 18:42:17 2015  
 Z,EapHost,@%systemroot%\system32\eapsvc.dll;-1,%SystemRoot%\System32\svchost.exe -k  
 netsvcs,Share\_Process,Manual,localSystem,@%systemroot%\system32\eapsvc.dll,-2  
 Fri Feb 20 18:42:17 2015 Z,terminpt,Microsoft Remote Desktop Input  
 Driver,\SystemRoot\system32\drivers\terminpt.sys,Kernel  
 driver,Manual,,@%SystemRoot%\system32\tcpipcfg.dll,-50004  
 Fri Feb 20 18:42:17 2015 Z,TsUsbGD,Remote Desktop Generic USB  
 Device,\SystemRoot\system32\drivers\TsUsbGD.sys,Kernel  
 driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000  
 Fri Feb 20 18:23:16 2015 Z,cphs,Intel(R) Content Protection HECI  
 Service,%SystemRoot%\SysWow64\IntelCpHeciSvc.exe,Own\_Process,Manual,LocalSystem,Inte  
 l(R) Content Protection HECI Service - enables communication with the Content  
 Protection FW  
 Fri Feb 20 18:22:35 2015  
 Z,{FD2B5103-617C-4AE6-8DC4-A4772C463DDC},,,,,@%SystemRoot%\System32\wwansvc.dll,-25  
 8  
 Fri Feb 20 17:05:34 2015 Z,vcsFPSservice,Validity VCS Fingerprint  
 Service,C:\Windows\system32\vcsFPSservice.exe,Own\_Process,Auto  
 Start,LocalSystem,Validity Fingerprint Service  
 Fri Feb 20 16:54:33 2015 Z,AtiHDAudioService,AMD Function Driver for HD Audio  
 Service,system32\drivers\AtihdW76.sys,Kernel  
 driver,Manual,,@%systemroot%\system32\rascfg.dll,-32000  
 Fri Feb 20 16:54:27 2015 Z,amdkgmdap,,system32\DRIVERS\atikmpag.sys,Kernel  
 driver,Manual,,@%SystemRoot%\system32\Alg.exe,-113  
 Fri Feb 20 16:54:14 2015  
 Z,{3ED9F155-8201-430C-85E1-EDD7020DE0CF},,,,,@%SystemRoot%\System32\wwansvc.dll,-25  
 8  
 Fri Feb 20 16:53:55 2015 Z,AMD External Events  
 Utility,,%SystemRoot%\system32\atiesrxx.exe,Own\_Process,Auto  
 Start,LocalSystem,@%SystemRoot%\system32\Alg.exe,-113  
 Fri Feb 20 16:53:55 2015 Z,Atierecord,,,,,@%systemroot%\system32\rascfg.dll,-32000  
 Fri Feb 20 16:53:55 2015  
 Z,iphlpvc\Parameters,,%SystemRoot%\System32\iphlpvc.dll,,,,  
 Fri Feb 20 16:53:49 2015  
 Z,{8B32CCEF-F092-453D-A04B-084246668014},,,,,@%SystemRoot%\System32\wwansvc.dll,-25  
 8  
 Fri Feb 20 16:53:43 2015  
 Z,{749B2830-EBF4-4268-8BFD-189D3224ACFB},,,,,@%SystemRoot%\System32\wwansvc.dll,-25  
 8  
 Fri Feb 20 16:53:35 2015 Z,hpsrv,HP  
 Service,%SystemRoot%\system32\Hpsservice.exe,Own\_Process,Auto  
 Start,LocalSystem,Mcafee Home Network

## SYSTEM OUTPUT

Fri Feb 20 16:53:06 2015 Z,ohci1394,1394 OHCI Compliant Host Controller (Legacy),\SystemRoot\system32\drivers\ohci1394.sys,Kernel driver,Manual,,Run portions of Microsoft Office Diagnostics.

Mon Dec 1 14:38:46 2014  
 Z,SysMain,@%SystemRoot%\system32\sysmain.dll;-1000,%systemroot%\system32\svchost.exe -k LocalSystemNetworkRestricted,Share\_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\sysmain.dll,-1001

Mon Dec 1 14:16:45 2014  
 Z,WatAdminSvc,@%SystemRoot%\system32\Wat\WatUX.exe;-601,%SystemRoot%\system32\Wat\WatAdminSvc.exe,Own\_Process,Manual,LocalSystem,@%SystemRoot%\system32\Wat\WatUX.exe,-602

Mon Dec 1 14:14:27 2014 Z,gpsvc,@gpapi.dll;-112,%windir%\system32\svchost.exe -k GPSvcGroup,Own\_Process,Auto Start,LocalSystem,@gpapi.dll,-113

Mon Dec 1 14:13:22 2014  
 Z,IEEtwCollectorService,@%SystemRoot%\system32\ieetwcollectorres.dll;-1000,%SystemRoot%\system32\IEEtwCollector.exe /V,Own\_Process,Manual,LocalSystem,@%SystemRoot%\system32\ieetwcollectorres.dll,-1001

Mon Dec 1 14:13:22 2014  
 Z,RDPUDD,,,,,@%systemroot%\system32\drivers\RdpRefMp.sys,-100

Mon Dec 1 14:13:22 2014 Z,RdpVideoMiniport,Remote Desktop Video Miniport Driver,System32\drivers\rdpvideominiport.sys,Kernel driver,Manual,,@%systemroot%\system32\drivers\RdpRefMp.sys,-100

Mon Dec 1 14:13:22 2014 Z,WinHttpAutoProxySvc\Parameters,,winhttp.dll,,,,

Mon Dec 1 14:01:16 2014 Z,MSDTC Bridge 3.0.0.0,,,,,@comres.dll,-2798

Mon Dec 1 14:01:16 2014 Z,ServiceModelEndpoint 3.0.0.0,,,,,@%SystemRoot%\System32\sensrsvc.dll,-1001

Mon Dec 1 14:01:16 2014 Z,ServiceModelOperation 3.0.0.0,,,,,@%SystemRoot%\System32\sensrsvc.dll,-1001

Mon Dec 1 14:01:16 2014 Z,ServiceModelService 3.0.0.0,,,,,@%SystemRoot%\System32\sensrsvc.dll,-1001

Mon Dec 1 14:01:16 2014 Z,SMsvchost 3.0.0.0,,,,,@%SystemRoot%\system32\tcpipcfg.dll,-50006

Mon Dec 1 14:01:16 2014 Z,Windows Workflow Foundation 3.0.0.0,,,,,@ProgramFiles%\Windows Defender\MsMpRes.dll,-1176

Mon Dec 1 13:04:59 2014  
 Z,wuauerv,@%systemroot%\system32\wuaueng.dll;-105,%systemroot%\system32\svchost.exe -k netsvcs,Share\_Process,Auto Start,LocalSystem,@%systemroot%\system32\wuaueng.dll,-106

Mon Dec 1 13:00:30 2014 Z,Wlansvc\Parameters,,%SystemRoot%\System32\wlansvc.dll,,,,

Mon Dec 1 12:59:32 2014 Z,BTHPORT,Bluetooth Port Driver,System32\Drivers\BTHport.sys,Kernel driver,Manual,,Bluetooth Device (Personal Area Network)

Mon Dec 1 12:59:19 2014  
 Z,Wlansvc,@%SystemRoot%\System32\wlansvc.dll;-257,%SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted,Share\_Process,Auto Start,LocalSystem,@%SystemRoot%\System32\wlansvc.dll,-258

Sat Nov 29 16:11:45 2014  
 Z,WebClient,@%systemroot%\system32\webclnt.dll;-100,%SystemRoot%\system32\svchost.exe

## SYSTEM OUTPUT

```

e -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\webclnt.dll,-101
Sat Nov 29 16:10:13 2014 Z,ProfSvc\Parameters,,%systemroot%\system32\profsvc.dll,,,,
Sat Nov 29 16:10:13 2014
Z,WebClient\Parameters,,%SystemRoot%\System32\webclnt.dll,,,,
Sat Nov 29 16:07:24 2014
Z,wudfsvc,@%SystemRoot%\system32\wudfsvc.dll;-1000,%SystemRoot%\system32\svchost.exe
-k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\wudfsvc.dll,-1001
Sat Nov 29 16:06:59 2014
Z,FontCache,@%systemroot%\system32\FntCache.dll;-100,%SystemRoot%\system32\svchost.e
xe -k LocalService,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%systemroot%\system32\FntCache.dll,-101
Sat Nov 29 16:06:59 2014
Z,FontCache\Parameters,,%SystemRoot%\system32\FntCache.dll,,,,
Tue Apr 12 08:29:05 2011
Z,CscService,@%systemroot%\system32\cscsvc.dll;-200,%SystemRoot%\System32\svchost.ex
e -k LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%systemroot%\system32\cscsvc.dll,-201
Tue Apr 12 08:28:48 2011
Z,AppMgmt,@appmgmts.dll;-3250,%SystemRoot%\system32\svchost.exe -k
netsvcs,Share_Process,Manual,LocalSystem,@appmgmts.dll,-3251
Tue Apr 12 08:28:48 2011
Z,ehRecvr,@%SystemRoot%\ehome\ehrecvr.exe;-101,%systemroot%\ehome\ehRecvr.exe,Own_Pr
ocess,Manual,NT AUTHORITY\NetworkService,@%SystemRoot%\ehome\ehrecvr.exe,-102
Tue Apr 12 08:28:48 2011
Z,ehSched,@%SystemRoot%\ehome\ehsched.exe;-101,%systemroot%\ehome\ehsched.exe,Own_Pr
ocess,Manual,NT AUTHORITY\NetworkService,@%SystemRoot%\ehome\ehsched.exe,-102
Tue Apr 12 08:28:48 2011
Z,Mcx2Svc,@%SystemRoot%\ehome\ehres.dll;-15501,%SystemRoot%\system32\svchost.exe -k
LocalServiceAndNoImpersonation,Share_Process,Disabled,NT
Authority\LocalService,@%SystemRoot%\ehome\ehres.dll,-15502
Tue Apr 12 08:28:48 2011
Z,PeerDistSvc,@%SystemRoot%\system32\peerdistsvc.dll;-9000,%SystemRoot%\System32\svc
host.exe -k PeerDist,Share_Process,Manual,NT
AUTHORITY\NetworkService,@%SystemRoot%\system32\peerdistsvc.dll,-9001
Tue Apr 12 08:28:48 2011 Z,RDPDR,Terminal Server Device Redirector
Driver,System32\drivers\rdpdr.sys,Kernel
driver,Manual,,@%systemroot%\system32\DRIVERS\RDPCDD.sys,-101
Tue Apr 12 08:28:48 2011
Z,SensrSvc,@%SystemRoot%\System32\sensrsvc.dll;-1000,%SystemRoot%\system32\svchost.e
xe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\sensrsvc.dll,-1001
Tue Apr 12 08:28:48 2011
Z,StorSvc,@%SystemRoot%\System32\StorSvc.dll;-100,%SystemRoot%\System32\svchost.exe
-k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32

```

## SYSTEM OUTPUT

```

\StorSvc.dll,-101
Tue Apr 12 08:28:48 2011
Z,UmRdpService,@%SystemRoot%\system32\umrdp.dll;-1000,%SystemRoot%\System32\svchost.
exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,localSystem,@%SystemRoot%\system32
\umrdp.dll,-1001
Tue Apr 12 08:28:45 2011
Z,AppMgmt\Parameters,,%SystemRoot%\System32\appmgmts.dll,,,,
Tue Apr 12 08:28:45 2011
Z,CscService\Parameters,,%SystemRoot%\System32\cscsvc.dll,,,,
Tue Apr 12 08:28:45 2011 Z,Mcx2Svc\Parameters,,%SystemRoot%\system32\Mcx2Svc.dll,,,,
Tue Apr 12 08:28:45 2011
Z,PeerDistSvc\Parameters,,%SystemRoot%\system32\peerdistsvc.dll,,,,
Tue Apr 12 08:28:45 2011
Z,SensrSvc\Parameters,,%SystemRoot%\system32\sensrsvc.dll,,,,
Tue Apr 12 08:28:45 2011 Z,StorSvc\Parameters,,%SystemRoot%\system32\storsvc.dll,,,,
Tue Apr 12 08:28:45 2011
Z,UmRdpService\Parameters,,%SystemRoot%\System32\umrdp.dll,,,,
Tue Apr 12 08:27:52 2011 Z,dmrvsc,,\SystemRoot\system32\drivers\dmrvsc.sys,Kernel
driver,Manual,,@%systemroot%\system32\drivers\discache.sys,-101
Tue Apr 12 08:27:52 2011 Z,s3cap,,\SystemRoot\system32\drivers\vm3cap.sys,Kernel
driver,Manual,,@oleres.dll,-5011
Tue Apr 12 08:27:52 2011
Z,VBushID,,\SystemRoot\system32\drivers\VBushID.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\vds.exe,-112
Sun Nov 21 03:58:24 2010 Z,BTHMODEM,Bluetooth Serial Communications
Driver,\SystemRoot\system32\drivers\bthmodem.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-101
Sun Nov 21 03:58:22 2010 Z,gagp30kx,Microsoft Generic AGPv3.0 Filter for K8
Processor Platforms,\SystemRoot\system32\drivers\gagp30kx.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\fvevol.sys,-100
Sun Nov 21 03:58:22 2010 Z,uagp35,Microsoft AGPv3.5
Filter,\SystemRoot\system32\drivers\uagp35.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000
Sun Nov 21 03:58:21 2010 Z,b06bdrv,Broadcom NetXtreme II
VBD,\SystemRoot\system32\drivers\bxbvda.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\AxInstSV.dll,-104
Sun Nov 21 03:58:21 2010 Z,HidBth,Microsoft Bluetooth HID
Miniport,\SystemRoot\system32\drivers\hidbth.sys,Kernel driver,Manual,,Keeps your
Google software up to date. If this service is disabled or stopped, your Google
software will not be kept up to date, meaning security vulnerabilities that may
arise cannot be fixed and features may not work. This service uninstalls itself when
there is no Google software using it.
Sun Nov 21 03:58:19 2010 Z,AmdK8,AMD K8 Processor
Driver,\SystemRoot\system32\drivers\amdk8.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\Alg.exe,-113
Sun Nov 21 03:58:19 2010 Z,AmdPPM,AMD Processor
Driver,\SystemRoot\system32\drivers\amdppm.sys,Kernel

```

## SYSTEM OUTPUT

```

driver,Manual,,@%SystemRoot%\system32\Alg.exe,-113
Sun Nov 21 03:58:19 2010 Z,Processor,Processor
Driver,\SystemRoot\system32\drivers\processr.sys,Kernel
driver,Manual,,@%systemroot%\system32\rascfg.dll,-32006
Sun Nov 21 03:58:18 2010 Z,ebdrv,Broadcom NetXtreme II 10 GigE
VBD,\SystemRoot\system32\drivers\evbda.sys,Kernel
driver,Manual,,@%systemroot%\system32\eapsvc.dll,-2
Sun Nov 21 03:58:18 2010 Z,fdc,Floppy Disk Controller
Driver,\SystemRoot\system32\drivers\fdc.sys,Kernel
driver,Manual,,@%systemroot%\system32\fxsresm.dll,-122
Sun Nov 21 03:58:17 2010 Z,pcmcia,,\SystemRoot\system32\drivers\pcmcia.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\pcasvc.dll,-2
Sun Nov 21 03:58:16 2010 Z,MTConfig,Microsoft Input Configuration
Driver,\SystemRoot\system32\drivers\MTConfig.sys,Kernel driver,Manual,,This service
filters e-mail messages on your computer
Sun Nov 21 03:58:15 2010 Z,circlass,Consumer IR
Devices,\SystemRoot\system32\drivers\circlass.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\certprop.dll,-12
Sun Nov 21 03:58:13 2010 Z,flpydisk,Floppy Disk
Driver,\SystemRoot\system32\drivers\flpydisk.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\drivers\filetrace.sys,-10000
Sun Nov 21 03:58:13 2010 Z,sfloppy,High-Capacity Floppy Disk
Drive,\SystemRoot\system32\drivers\sfloppy.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\SessEnv.dll,-1027
Sun Nov 21 03:58:11 2010 Z,HidBatt,HID UPS Battery
Driver,\SystemRoot\system32\drivers\HidBatt.sys,Kernel driver,Manual,,Keeps your
Google software up to date. If this service is disabled or stopped, your Google
software will not be kept up to date, meaning security vulnerabilities that may
arise cannot be fixed and features may not work. This service uninstalls itself when
there is no Google software using it.
Sun Nov 21 03:58:08 2010 Z,HidIr,Microsoft Infrared HID
Driver,\SystemRoot\system32\drivers\hidir.sys,Kernel driver,Manual,,Keeps your
Google software up to date. If this service is disabled or stopped, your Google
software will not be kept up to date, meaning security vulnerabilities that may
arise cannot be fixed and features may not work. This service uninstalls itself when
there is no Google software using it.
Sun Nov 21 03:58:07 2010 Z,sermouse,Serial Mouse
Driver,\SystemRoot\system32\drivers\sermouse.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\sensrsvc.dll,-1001
Sun Nov 21 03:58:06 2010 Z,BrFiltLo,Brother USB Mass-Storage Lower Filter
Driver,\SystemRoot\system32\drivers\BrFiltLo.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-103
Sun Nov 21 03:58:06 2010 Z,BrFiltUp,Brother USB Mass-Storage Upper Filter
Driver,\SystemRoot\system32\drivers\BrFiltUp.sys,Kernel
driver,Manual,,@%systemroot%\system32\browser.dll,-103
Sun Nov 21 03:58:05 2010 Z,usbohci,Microsoft USB Open Host Controller Miniport
Driver,\SystemRoot\system32\drivers\usbohci.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214

```

## SYSTEM OUTPUT

Sun Nov 21 03:58:05 2010 Z,usbuhci,Microsoft USB Universal Host Controller Miniport Driver,\SystemRoot\system32\drivers\usbuhci.sys,Kernel driver,Manual,,@%systemroot%\system32\upnphost.dll,-214

Sun Nov 21 03:58:00 2010 Z,WacomPen,Wacom Serial Pen HID Driver,\SystemRoot\system32\drivers\wacompen.sys,Kernel driver,Manual,,@%SystemRoot%\system32\w32time.dll,-201

Sun Nov 21 03:57:59 2010 Z,crcdisk,Crcdisk Filter Driver,\SystemRoot\system32\drivers\crcdisk.sys,Kernel driver,Disabled,,Intel(R) Content Protection HECI Service - enables communication with the Content Protection FW

Sun Nov 21 03:57:58 2010 Z,UmPass,Microsoft UMPass Driver,\SystemRoot\system32\drivers\umpass.sys,Kernel driver,Manual,,@%SystemRoot%\system32\ui0detect.exe,-102

Sun Nov 21 03:46:56 2010 Z,b57nd60a,Broadcom NetXtreme Gigabit Ethernet - NDIS 6.0,system32\DRIVERS\b57nd60a.sys,Kernel driver,Manual,,@%SystemRoot%\system32\AxInstSV.dll,-104

Sun Nov 21 03:46:56 2010 Z,vga,,system32\DRIVERS\vgapnp.sys,Kernel driver,Manual,,@%SystemRoot%\system32\vds.exe,-112

Sun Nov 21 03:39:53 2010 Z,Dhcp\Parameters,,%SystemRoot%\system32\dhcpcore.dll,,,

Sun Nov 21 03:38:46 2010 Z,TsUsbFlt,,system32\drivers\tsusbflt.sys,Kernel driver,Manual,,@%SystemRoot%\system32\drivers\tsusbflt.sys,-1000

Sun Nov 21 03:33:56 2010 Z,SessionEnv,@%SystemRoot%\System32\SessEnv.dll;-1026,%SystemRoot%\System32\svchost.exe -k

netshvcs,Share\_Process,Manual,localSystem,@%SystemRoot%\System32\SessEnv.dll,-1027

Sun Nov 21 03:29:32 2010 Z,AcpiPmi,ACPI Power Meter Driver,\SystemRoot\system32\drivers\acpipmi.sys,Kernel driver,Manual,,@%SystemRoot%\System32\wwansvc.dll,-258

Sun Nov 21 03:29:32 2010 Z,agp440,Intel AGP Bus Filter,\SystemRoot\system32\drivers\agp440.sys,Kernel driver,Manual,,@%systemroot%\system32\drivers\afd.sys,-1000

Sun Nov 21 03:29:32 2010 Z,amdxdta,,system32\drivers\amdxdta.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\Alg.exe,-113

Sun Nov 21 03:29:32 2010 Z,ErrDev,Microsoft Hardware Error Device Driver,\SystemRoot\system32\drivers\errdev.sys,Kernel driver,Manual,,@%SystemRoot%\ehome\ehsched.exe,-102

Sun Nov 21 03:29:32 2010 Z,IPMIDRV,,\SystemRoot\system32\drivers\IPMIDrv.sys,Kernel driver,Manual,,@%SystemRoot%\system32\iphlpvc.dll,-501

Sun Nov 21 03:29:32 2010 Z,iScsiPrt,iScsiPort Driver,\SystemRoot\system32\drivers\msiscsi.sys,Kernel driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101

Sun Nov 21 03:29:32 2010 Z,nv\_agp,NVIDIA nForce AGP Bus Filter,\SystemRoot\system32\drivers\nv\_agp.sys,Kernel driver,Manual,,@%SystemRoot%\system32\drivers\nsiproxy.sys,-1

Sun Nov 21 03:29:32 2010 Z,sffdisk,SFF Storage Class Driver,\SystemRoot\system32\drivers\sffdisk.sys,Kernel driver,Manual,,@%SystemRoot%\System32\SessEnv.dll,-1027

Sun Nov 21 03:29:32 2010 Z,sffp\_mmc,SFF Storage Protocol Driver for

## SYSTEM OUTPUT

```

MMC,\SystemRoot\system32\drivers\sffp_mmc.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\SessEnv.dll,-1027
Sun Nov 21 03:29:32 2010 Z,sffp_sd,SFF Storage Protocol Driver for
SDBus,\SystemRoot\system32\drivers\sffp_sd.sys,Kernel
driver,Manual,,@%SystemRoot%\System32\SessEnv.dll,-1027
Sun Nov 21 03:29:32 2010 Z,uliagpkx,Uli AGP Bus
Filter,\SystemRoot\system32\drivers\uliagpkx.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\ui0detect.exe,-102
Sun Nov 21 03:29:32 2010 Z,usbcir,eHome Infrared Receiver
(USBCIR),\SystemRoot\system32\drivers\usbcir.sys,Kernel
driver,Manual,,@%systemroot%\system32\upnphost.dll,-214
Sun Nov 21 03:29:32 2010 Z,vhdmf,\SystemRoot\system32\drivers\vhdmf.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\vds.exe,-112
Tue Jul 14 05:34:12 2009 Z,BDESVC\Parameters,,%SystemRoot%\System32\bdesvc.dll,,,,
Tue Jul 14 05:34:12 2009
Z,PNRPAutoReg\Parameters,,%SystemRoot%\system32\pnrpauto.dll,,,,
Tue Jul 14 05:34:12 2009 Z,WPCSvc\Parameters,,%SystemRoot%\System32\wpcsvc.dll,,,,
Tue Jul 14 05:34:09 2009
Z,p2pimsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,,
Tue Jul 14 05:34:09 2009 Z,p2psvc\Parameters,,%SystemRoot%\system32\p2psvc.dll,,,,
Tue Jul 14 05:34:09 2009 Z,SDRSVC\Parameters,,%Systemroot%\System32\SDRSVC.dll,,,,
Tue Jul 14 04:54:38 2009 Z,NdisCap,NDIS Capture Lightweight
Filter,system32\DRIVERS\ndiscap.sys,Kernel driver,Manual,,NDIS Capture Lightweight
Filter
Tue Jul 14 04:54:32 2009 Z,hkmsvc\Parameters,,%SystemRoot%\system32\kmsvc.dll,,,,
Tue Jul 14 04:54:31 2009
Z,napagent\Parameters,,%SystemRoot%\system32\qagentRT.dll,,,,
Tue Jul 14 04:54:25 2009
Z,defragsvc\Parameters,,%Systemroot%\System32\defragsvc.dll,,,,
Tue Jul 14 04:54:05 2009 Z,WerSvc\Parameters,,%SystemRoot%\System32\WerSvc.dll,,,,
Tue Jul 14 04:53:57 2009
Z,Smb,@%SystemRoot%\system32\tcpipcfg.dll;-50005,system32\DRIVERS\smb.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\tcpipcfg.dll,-50006
Tue Jul 14 04:53:56 2009 Z,lmhosts\Parameters,,%SystemRoot%\System32\lmhsvc.dll,,,,
Tue Jul 14 04:53:48 2009
Z,THREADORDER\Parameters,,%SystemRoot%\system32\mmcscs.dll,,,,
Tue Jul 14 04:53:45 2009
Z,TrkWks,@%SystemRoot%\system32\trkwks.dll;-1,%SystemRoot%\System32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\trkwks.dll,-2
Tue Jul 14 04:53:45 2009 Z,TrkWks\Parameters,,%SystemRoot%\System32\trkwks.dll,,,,
Tue Jul 14 04:53:36 2009
Z,RpcEptMapper,@%windir%\system32\RpcEpMap.dll;-1001,%SystemRoot%\system32\svchost.e
xe -k RPCSS,Share_Process,Auto Start,NT
AUTHORITY\NetworkService,@%windir%\system32\RpcEpMap.dll,-1002
Tue Jul 14 04:53:36 2009
Z,RpcEptMapper\Parameters,,%SystemRoot%\System32\RpcEpMap.dll,,,,
Tue Jul 14 04:53:33 2009

```



## SYSTEM OUTPUT

Z,LanmanServer,@%systemroot%\system32\svcsvc.dll;-100,%SystemRoot%\system32\svchost.exe -k netsvcs,Share\_Process,Auto Start,LocalSystem,@%systemroot%\system32\svcsvc.dll,-101  
 Tue Jul 14 04:53:31 2009  
 Z,LanmanWorkstation,@%systemroot%\system32\wkssvc.dll;-100,%SystemRoot%\System32\svchost.exe -k NetworkService,Share\_Process,Auto Start,NT AUTHORITY\NetworkService,@%systemroot%\system32\wkssvc.dll,-101  
 Tue Jul 14 04:53:31 2009  
 Z,LanmanWorkstation\Parameters,,%SystemRoot%\System32\wkssvc.dll,,,,  
 Tue Jul 14 04:53:25 2009 Z,WmiApRpl,,,,,@%SystemRoot%\System32\wlansvc.dll,-258  
 Tue Jul 14 04:53:24 2009  
 Z,Wingmt,@%Systemroot%\system32\wbem\wmisvc.dll;-205,%systemroot%\system32\svchost.exe -k netsvcs,Share\_Process,Auto Start,localSystem,@%Systemroot%\system32\wbem\wmisvc.dll,-204  
 Tue Jul 14 04:53:24 2009  
 Z,wmiApSrv,@%Systemroot%\system32\wbem\wmiapsrv.exe;-110,%systemroot%\system32\wbem\WmiApSrv.exe,Own\_Process,Manual,localSystem,@%Systemroot%\system32\wbem\wmiapsrv.exe,-111  
 Tue Jul 14 04:53:21 2009 Z,TCPIP6,Microsoft IPv6 Protocol Driver,system32\DRIVERS\tcpip.sys,Kernel driver,Manual,,Microsoft IPv6 Protocol Driver  
 Tue Jul 14 04:53:21 2009  
 Z,WANARP,@%systemroot%\system32\rascfg.dll;-32011,system32\DRIVERS\wanarp.sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32011  
 Tue Jul 14 04:53:20 2009  
 Z,lmhosts,@%SystemRoot%\system32\lmhsvc.dll;-101,%SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted,Share\_Process,Auto Start,NT AUTHORITY\LocalService,@%SystemRoot%\system32\lmhsvc.dll,-102  
 Tue Jul 14 04:53:19 2009  
 Z,Dhcp,@%SystemRoot%\system32\dhcpcore.dll;-100,%SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted,Share\_Process,Auto Start,NT Authority\LocalService,@%SystemRoot%\system32\dhcpcore.dll,-101  
 Tue Jul 14 04:53:19 2009  
 Z,Winsock,,Adapter,Manual,,@%Systemroot%\system32\wsmsvc.dll,-102  
 Tue Jul 14 04:49:48 2009  
 Z,SamSs,@%SystemRoot%\system32\samsrv.dll;-1,%SystemRoot%\system32\lsass.exe,Share\_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\samsrv.dll,-2  
 Tue Jul 14 04:49:48 2009  
 Z,W32Time,@%SystemRoot%\system32\w32time.dll;-200,%SystemRoot%\system32\svchost.exe -k LocalService,Share\_Process,Manual,NT AUTHORITY\LocalService,@%SystemRoot%\system32\w32time.dll,-201  
 Tue Jul 14 04:49:48 2009 Z,W32Time\Parameters,,%systemroot%\system32\w32time.dll,,,,  
 Tue Jul 14 04:49:46 2009  
 Z,Dnscache,@%SystemRoot%\System32\dnsapi.dll;-101,%SystemRoot%\system32\svchost.exe -k NetworkService,Share\_Process,Auto Start,NT AUTHORITY\NetworkService,@%SystemRoot%\System32\dnsapi.dll,-102  
 Tue Jul 14 04:49:46 2009  
 Z,Dnscache\Parameters,,%SystemRoot%\System32\dnsrslvr.dll,,,,

## SYSTEM OUTPUT

```

Tue Jul 14 04:49:45 2009
Z,RemoteAccess,@%Systemroot%\system32\mprdim.dll;-200,%SystemRoot%\System32\svchost.exe -k
netsvcs,Share_Process,Disabled,localSystem,@%Systemroot%\system32\mprdim.dll,-201
Tue Jul 14 04:49:45 2009
Z,RemoteAccess\Parameters,,%SystemRoot%\System32\mprdim.dll,,,
Tue Jul 14 04:49:35 2009
Z,RasAuto,@%Systemroot%\system32\rasauto.dll;-200,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Manual,localSystem,@%Systemroot%\system32\rasauto.dll,-201
Tue Jul 14 04:49:35 2009 Z,RasAuto\Parameters,,%SystemRoot%\System32\rasauto.dll,,,
Tue Jul 14 04:49:35 2009
Z,RasMan,@%Systemroot%\system32\rasmans.dll;-200,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Manual,localSystem,@%Systemroot%\system32\rasmans.dll,-201
Tue Jul 14 04:49:35 2009 Z,RasMan\Parameters,,%SystemRoot%\System32\rasmans.dll,,,
Tue Jul 14 04:49:26 2009 Z,SstpSvc\Parameters,,%SystemRoot%\system32\sstpsvc.dll,,,
Tue Jul 14 04:49:24 2009
Z,DPS,@%systemroot%\system32\dps.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Auto Start,NT
AUTHORITY\LocalService,@%systemroot%\system32\dps.dll,-501
Tue Jul 14 04:49:24 2009 Z,DPS\Parameters,,%SystemRoot%\system32\dps.dll,,,
Tue Jul 14 04:49:24 2009
Z,WdiServiceHost,@%systemroot%\system32\wdi.dll;-502,%SystemRoot%\System32\svchost.e
xe -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\wdi.dll,-503
Tue Jul 14 04:49:24 2009
Z,WdiServiceHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Tue Jul 14 04:49:24 2009
Z,WdiSystemHost,@%systemroot%\system32\wdi.dll;-500,%SystemRoot%\System32\svchost.ex
e -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%systemroot%\system32
\wdi.dll,-501
Tue Jul 14 04:49:24 2009
Z,WdiSystemHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Tue Jul 14 04:49:23 2009 Z,EapHost\Parameters,,%SystemRoot%\System32\eapsvc.dll,,,
Tue Jul 14 04:49:20 2009 Z,gpsvc\Parameters,,%SystemRoot%\System32\gpsvc.dll,,,
Tue Jul 14 04:49:20 2009 Z,NlaSvc\Parameters,,%SystemRoot%\System32\nlasvc.dll,,,
Tue Jul 14 04:49:18 2009 Z,BITS\Parameters,,%SystemRoot%\System32\qmgr.dll,,,
Tue Jul 14 04:49:08 2009 Z,nsi\Parameters,,%systemroot%\system32\nsisvc.dll,,,
Tue Jul 14 04:49:01 2009 Z,.NET CLR
Data,,,,,%SystemRoot%\System32\wwansvc.dll,-258
Tue Jul 14 04:49:01 2009 Z,.NET CLR
Networking,,,,,%SystemRoot%\System32\wwansvc.dll,-258
Tue Jul 14 04:49:01 2009 Z,.NET Data Provider for
Oracle,,,,,%SystemRoot%\System32\wwansvc.dll,-258
Tue Jul 14 04:49:01 2009 Z,.NET Data Provider for
SqlServer,,,,,%SystemRoot%\System32\wwansvc.dll,-258
Tue Jul 14 04:49:01 2009
Z,.NETFramework,,,,,%SystemRoot%\System32\wwansvc.dll,-258

```

## SYSTEM OUTPUT

Tue Jul 14 04:49:01 2009 Z,adsi,,,,,@%SystemRoot%\System32\wwansvc.dll,-258  
 Tue Jul 14 04:49:01 2009  
 Z,AeLookupSvc,@%SystemRoot%\system32\aelupsvc.dll;-1,%systemroot%\system32\svchost.exe -k  
 netsvcs,Share\_Process,Manual,localSystem,@%SystemRoot%\system32\aelupsvc.dll,-2  
 Tue Jul 14 04:49:01 2009  
 Z,AeLookupSvc\Parameters,,%SystemRoot%\System32\aelupsvc.dll,,,  
 Tue Jul 14 04:49:01 2009  
 Z,ALG,@%SystemRoot%\system32\Alg.exe;-112,%SystemRoot%\System32\alg.exe,Own\_Process,Manual,NT AUTHORITY\LocalService,@%SystemRoot%\system32\Alg.exe,-113  
 Tue Jul 14 04:49:01 2009  
 Z,AppID,@%systemroot%\system32\appidsvc.dll;-102,\SystemRoot\system32\drivers\appid.sys,Kernel driver,Manual,,@%systemroot%\system32\appidsvc.dll,-103  
 Tue Jul 14 04:49:01 2009  
 Z,AppIDSvc,@%systemroot%\system32\appidsvc.dll;-100,%SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation,Share\_Process,Manual,NT Authority\LocalService,@%systemroot%\system32\appidsvc.dll,-101  
 Tue Jul 14 04:49:01 2009  
 Z,AppIDSvc\Parameters,,%SystemRoot%\System32\appidsvc.dll,,,  
 Tue Jul 14 04:49:01 2009  
 Z,Appinfo,@%systemroot%\system32\appinfo.dll;-100,%SystemRoot%\system32\svchost.exe -k netsvcs,Share\_Process,Manual,LocalSystem,@%systemroot%\system32\appinfo.dll,-101  
 Tue Jul 14 04:49:01 2009 Z,Appinfo\Parameters,,%SystemRoot%\System32\appinfo.dll,,,  
 Tue Jul 14 04:49:01 2009  
 Z,AudioEndpointBuilder,@%SystemRoot%\system32\audiosrv.dll;-204,%SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted,Share\_Process,Auto Start,LocalSystem,@%SystemRoot%\System32\audiosrv.dll,-205  
 Tue Jul 14 04:49:01 2009  
 Z,AudioEndpointBuilder\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,  
 Tue Jul 14 04:49:01 2009  
 Z,AudioSrv,@%SystemRoot%\system32\audiosrv.dll;-200,%SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted,Share\_Process,Auto Start,NT AUTHORITY\LocalService,@%SystemRoot%\System32\audiosrv.dll,-201  
 Tue Jul 14 04:49:01 2009  
 Z,AudioSrv\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,  
 Tue Jul 14 04:49:01 2009  
 Z,AxInstSV,@%SystemRoot%\system32\AxInstSV.dll;-103,%SystemRoot%\system32\svchost.exe -k  
 AxInstSVGroup,Share\_Process,Manual,LocalSystem,@%SystemRoot%\system32\AxInstSV.dll,-104  
 Tue Jul 14 04:49:01 2009  
 Z,AxInstSV\Parameters,,%SystemRoot%\System32\AxInstSV.dll,,,  
 Tue Jul 14 04:49:01 2009 Z,BattC,,,,,@%SystemRoot%\system32\AxInstSV.dll,-104  
 Tue Jul 14 04:49:01 2009  
 Z,BDESVC,@%SystemRoot%\system32\bdesvc.dll;-100,%SystemRoot%\System32\svchost.exe -k netsvcs,Share\_Process,Manual,localSystem,@%SystemRoot%\system32\bdesvc.dll,-101  
 Tue Jul 14 04:49:01 2009  
 Z,BFE,@%SystemRoot%\system32\bfe.dll;-1001,%systemroot%\system32\svchost.exe -k

## SYSTEM OUTPUT

LocalServiceNoNetwork,Share\_Process,Auto Start,NT  
 AUTHORITY\LocalService,@%SystemRoot%\system32\bfe.dll,-1002  
 Tue Jul 14 04:49:01 2009 Z,BFE\Parameters,,%SystemRoot%\System32\bfe.dll,,,,  
 Tue Jul 14 04:49:01 2009  
 Z,Browser,@%systemroot%\system32\browser.dll;-100,%SystemRoot%\System32\svchost.exe  
 -k netsvcs,Share\_Process,Manual,LocalSystem,@%systemroot%\system32\browser.dll,-101  
 Tue Jul 14 04:49:01 2009 Z,Browser\Parameters,,%SystemRoot%\System32\browser.dll,,,,  
 Tue Jul 14 04:49:01 2009 Z,Brserid,Brother MFC Serial Port Interface Driver  
 (WDM),\SystemRoot\System32\Drivers\Brserid.sys,Kernel  
 driver,Manual,,@%systemroot%\system32\browser.dll,-101  
 Tue Jul 14 04:49:01 2009 Z,BrSerWdm,Brother WDM Serial  
 driver,\SystemRoot\System32\Drivers\BrSerWdm.sys,Kernel  
 driver,Manual,,@%systemroot%\system32\browser.dll,-101  
 Tue Jul 14 04:49:01 2009 Z,BrUsbMdm,Brother MFC USB Fax Only  
 Modem,\SystemRoot\System32\Drivers\BrUsbMdm.sys,Kernel  
 driver,Manual,,@%systemroot%\system32\browser.dll,-101  
 Tue Jul 14 04:49:01 2009 Z,BrUsbSer,Brother MFC USB Serial WDM  
 Driver,\SystemRoot\System32\Drivers\BrUsbSer.sys,Kernel  
 driver,Manual,,@%systemroot%\system32\browser.dll,-101  
 Tue Jul 14 04:49:01 2009  
 Z,bthserv,@%SystemRoot%\System32\bthserv.dll;-101,%SystemRoot%\system32\svchost.exe  
 -k bthsvcs,Share\_Process,Manual,NT  
 AUTHORITY\LocalService,@%SystemRoot%\System32\bthserv.dll,-102  
 Tue Jul 14 04:49:01 2009 Z,bthserv\Parameters,,%SystemRoot%\system32\bthserv.dll,,,,  
 Tue Jul 14 04:49:01 2009  
 Z,CertPropSvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,,  
 Tue Jul 14 04:49:01 2009  
 Z,COMSysApp,@comres.dll;-947,%SystemRoot%\system32\dlhhost.exe  
 /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235},Own\_Process,Manual,LocalSystem,@co  
 mres.dll,-948  
 Tue Jul 14 04:49:01 2009 Z,crypt32,,,,,Intel(R) Content Protection HECI Service -  
 enables communication with the Content Protection FW  
 Tue Jul 14 04:49:01 2009  
 Z,CryptSvc,@%SystemRoot%\system32\cryptsvc.dll;-1001,%SystemRoot%\system32\svchost.e  
 xe -k NetworkService,Share\_Process,Auto Start,NT  
 Authority\NetworkService,@%SystemRoot%\system32\cryptsvc.dll,-1002  
 Tue Jul 14 04:49:01 2009  
 Z,CryptSvc\Parameters,,%SystemRoot%\system32\cryptsvc.dll,,,,  
 Tue Jul 14 04:49:01 2009 Z,DCLocator,,,,,@%systemroot%\system32\cscsvc.dll,-201  
 Tue Jul 14 04:49:01 2009  
 Z,DcomLaunch,@oleres.dll;-5012,%SystemRoot%\system32\svchost.exe -k  
 DcomLaunch,Share\_Process,Auto Start,LocalSystem,@oleres.dll,-5013  
 Tue Jul 14 04:49:01 2009  
 Z,defragSvc,@%SystemRoot%\system32\defragSvc.dll;-101,%SystemRoot%\system32\svchost.  
 exe -k  
 defragSvc,Own\_Process,Manual,localSystem,@%SystemRoot%\system32\defragSvc.dll,-102  
 Tue Jul 14 04:49:01 2009  
 Z,dot3svc,@%systemroot%\system32\dot3svc.dll;-1102,%SystemRoot%\system32\svchost.exe

## SYSTEM OUTPUT

-k

LocalSystemNetworkRestricted,Share\_Process,Manual,localSystem,@%systemroot%\system32\dot3svc.dll,-1103

Tue Jul 14 04:49:01 2009 Z,dot3svc\Parameters,,%SystemRoot%\System32\dot3svc.dll,,,

Tue Jul 14 04:49:01 2009

Z,EFS,@%SystemRoot%\system32\efssvc.dll;-100,%SystemRoot%\System32\lsass.exe,Share\_Process,Manual,LocalSystem,@%SystemRoot%\system32\efssvc.dll,-101

Tue Jul 14 04:49:01 2009 Z,ESENT,,,,,@%SystemRoot%\ehome\ehsched.exe,-102

Tue Jul 14 04:49:01 2009

Z,EventSystem,@comres.dll;-2450,%SystemRoot%\system32\svchost.exe -k

LocalService,Share\_Process,Auto Start,NT AUTHORITY\LocalService,@comres.dll,-2451

Tue Jul 14 04:49:01 2009 Z,EventSystem\Parameters,,%systemroot%\system32\es.dll,,,

Tue Jul 14 04:49:01 2009

Z,Fax,@%systemroot%\system32\fxsresm.dll;-118,%systemroot%\system32\fxssvc.exe,Own\_Process,Manual,NT AUTHORITY\NetworkService,@%systemroot%\system32\fxsresm.dll,-122

Tue Jul 14 04:49:01 2009

Z,fdPHost,@%systemroot%\system32\fdPHost.dll;-100,%SystemRoot%\system32\svchost.exe

-k LocalService,Share\_Process,Manual,NT

AUTHORITY\LocalService,@%systemroot%\system32\fdPHost.dll,-101

Tue Jul 14 04:49:01 2009 Z,fdPHost\Parameters,,%SystemRoot%\system32\fdPHost.dll,,,

Tue Jul 14 04:49:01 2009

Z,FDResPub\Parameters,,%SystemRoot%\system32\fdrespub.dll,,,

Tue Jul 14 04:49:01 2009

Z,Filetrace,@%SystemRoot%\system32\drivers\filetrace.sys;-10001,system32\drivers\filetrace.sys,File system

driver,Manual,,@%SystemRoot%\system32\drivers\filetrace.sys,-10000

Tue Jul 14 04:49:01 2009

Z,FontCache3.0.0.0,@%SystemRoot%\system32\PresentationHost.exe;-3309,%systemroot%\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe,Own\_Process,Manual,NT

Authority\LocalService,@%SystemRoot%\system32\PresentationHost.exe,-3310

Tue Jul 14 04:49:01 2009

Z,FsDepends,@%SystemRoot%\system32\drivers\fsdepends.sys;-10001,system32\drivers\FsDepends.sys,File system

driver,Manual,,@%SystemRoot%\system32\drivers\fsdepends.sys,-10000

Tue Jul 14 04:49:01 2009 Z,hcw85cir,Hauppauge Consumer Infrared

Receiver,\SystemRoot\system32\drivers\hcw85cir.sys,Kernel driver,Manual,,Keeps your Google software up to date. If this service is disabled or stopped, your Google software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This service uninstalls itself when there is no Google software using it.

Tue Jul 14 04:49:01 2009

Z,hidserv,@%SystemRoot%\System32\hidserv.dll;-101,%SystemRoot%\system32\svchost.exe -k

LocalSystemNetworkRestricted,Share\_Process,Manual,LocalSystem,@%SystemRoot%\System32\hidserv.dll,-102

Tue Jul 14 04:49:01 2009 Z,hidserv\Parameters,,%SystemRoot%\system32\hidserv.dll,,,

Tue Jul 14 04:49:01 2009

Z,hkmsvc,@%SystemRoot%\system32\kmsvc.dll;-6,%SystemRoot%\System32\svchost.exe -k

## SYSTEM OUTPUT

```

netsvcs,Share_Process,Manual,localSystem,@%SystemRoot%\system32\kmsvc.dll,-7
Tue Jul 14 04:49:01 2009
Z,HomeGroupListener\Parameters,,%SystemRoot%\system32\ListSvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,HomeGroupProvider,@%SystemRoot%\System32\provsvc.dll;-100,%SystemRoot%\System32\sv
chost.exe -k LocalServiceNetworkRestricted,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\System32\provsvc.dll,-101
Tue Jul 14 04:49:01 2009
Z,HomeGroupProvider\Parameters,,%SystemRoot%\system32\provsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,idsvc,@%systemroot%\Microsoft.NET\Framework64\v3.0\Windows Communication
Foundation\ServiceModelInstallRC.dll;-8193,"%systemroot%\Microsoft.NET\Framework64\v
3.0\Windows Communication
Foundation\infocard.exe",Share_Process,Manual,LocalSystem,@%systemroot%\Microsoft.NE
T\Framework64\v3.0\Windows Communication Foundation\ServiceModelInstallRC.dll,-8192
Tue Jul 14 04:49:01 2009 Z,IKEEXT\Parameters,,%SystemRoot%\System32\ikeext.dll,,,,
Tue Jul 14 04:49:01 2009 Z,inetaccs,,,,,@%SystemRoot%\system32\ikeext.dll,-502
Tue Jul 14 04:49:01 2009
Z,IPBusEnum,@%systemroot%\system32\IPBusEnum.dll;-102,%SystemRoot%\system32\svchost.
exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%systemroot%\system32
\IPBusEnum.dll,-103
Tue Jul 14 04:49:01 2009
Z,IPBusEnum\Parameters,,%SystemRoot%\system32\ipbusenum.dll,,,,
Tue Jul 14 04:49:01 2009
Z,IpFilterDriver,@%systemroot%\system32\rascfg.dll;-32013,system32\DRIVERS\ipfltdrv.
sys,Kernel driver,Manual,,@%systemroot%\system32\rascfg.dll,-32013
Tue Jul 14 04:49:01 2009
Z,iphlpvc,@%SystemRoot%\system32\iphlpvc.dll;-500,%SystemRoot%\System32\svchost.ex
e -k NetSvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\iphlpvc.dll,-501
Tue Jul 14 04:49:01 2009 Z,IPNAT,IP Network Address
Translator,System32\drivers\ipnat.sys,Kernel
driver,Manual,,@%SystemRoot%\system32\iphlpvc.dll,-501
Tue Jul 14 04:49:01 2009
Z,IENUM,@%SystemRoot%\system32\drivers\irenum.sys;-100,system32\drivers\irenum.sys,
Kernel driver,Manual,,@%SystemRoot%\system32\drivers\irenum.sys,-101
Tue Jul 14 04:49:01 2009
Z,KeyIso,@keyiso.dll;-100,%SystemRoot%\system32\lsass.exe,Share_Process,Manual,Local
System,@keyiso.dll,-101
Tue Jul 14 04:49:01 2009 Z,KtmRm,@comres.dll;-2946,%SystemRoot%\System32\svchost.exe
-k NetworkServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\NetworkService,@comres.dll,-2947
Tue Jul 14 04:49:01 2009 Z,KtmRm\Parameters,,%systemroot%\system32\msdtckrm.dll,,,,
Tue Jul 14 04:49:01 2009 Z,ldap,,,,,@%systemroot%\system32\wkssvc.dll,-101
Tue Jul 14 04:49:01 2009
Z,lltdsvc,@%SystemRoot%\system32\lltdres.dll;-1,%SystemRoot%\System32\svchost.exe -k
LocalService,Share_Process,Manual,NT

```

## SYSTEM OUTPUT

AUTHORITY\LocalService,@%SystemRoot%\system32\lltdres.dll,-2  
 Tue Jul 14 04:49:01 2009 Z,lltdsvc\Parameters,,%SystemRoot%\System32\lltdsvc.dll,,,,  
 Tue Jul 14 04:49:01 2009 Z,Lsa,,,,,@%SystemRoot%\system32\lmhsvc.dll,-102  
 Tue Jul 14 04:49:01 2009  
 Z,MMCSS,@%systemroot%\system32\mmcscs.dll;-100,%SystemRoot%\system32\svchost.exe -k  
 netsvcs,Share\_Process,Auto Start,LocalSystem,@%systemroot%\system32\mmcscs.dll,-101  
 Tue Jul 14 04:49:01 2009 Z,MMCSS\Parameters,,%SystemRoot%\system32\mmcscs.dll,,,,  
 Tue Jul 14 04:49:01 2009  
 Z,MpsSvc,@%SystemRoot%\system32\FirewallAPI.dll;-23090,%SystemRoot%\system32\svchost  
 .exe -k LocalServiceNoNetwork,Share\_Process,Auto Start,NT  
 Authority\LocalService,@%SystemRoot%\system32\FirewallAPI.dll,-23091  
 Tue Jul 14 04:49:01 2009 Z,MpsSvc\Parameters,,%SystemRoot%\system32\mpsSvc.dll,,,,  
 Tue Jul 14 04:49:01 2009  
 Z,MRxDAV,@%systemroot%\system32\webclnt.dll;-104,\SystemRoot\system32\drivers\mrxdav  
 .sys,File system driver,Manual,,@%systemroot%\system32\webclnt.dll,-105  
 Tue Jul 14 04:49:01 2009  
 Z,MSDTC,@comres.dll;-2797,%SystemRoot%\System32\msdtc.exe,Own\_Process,Manual,NT  
 AUTHORITY\NetworkService,@comres.dll,-2798  
 Tue Jul 14 04:49:01 2009  
 Z,mshidkmdf,@%SystemRoot%\system32\drivers\mshidkmdf.sys;-100,\SystemRoot\System32\drivers\mshidkmdf.sys,Kernel  
 driver,Manual,,@%SystemRoot%\system32\drivers\mshidkmdf.sys,-101  
 Tue Jul 14 04:49:01 2009  
 Z,MSiSCSI,@%SystemRoot%\system32\iscsidsc.dll;-5000,%systemroot%\system32\svchost.exe  
 e -k  
 netsvcs,Share\_Process,Manual,LocalSystem,@%SystemRoot%\system32\iscsidsc.dll,-5001  
 Tue Jul 14 04:49:01 2009  
 Z,MSiSCSI\Parameters,,%systemroot%\system32\iscsiexe.dll,,,,  
 Tue Jul 14 04:49:01 2009 Z,MsRPC,,,Kernel driver,Manual,,This service filters e-mail  
 messages on your computer  
 Tue Jul 14 04:49:01 2009 Z,MSSCNTRS,,,,,This service filters e-mail messages on  
 your computer  
 Tue Jul 14 04:49:01 2009  
 Z,napagent,@%SystemRoot%\system32\qagentrt.dll;-6,%SystemRoot%\System32\svchost.exe  
 -k NetworkService,Share\_Process,Manual,NT  
 AUTHORITY\NetworkService,@%SystemRoot%\system32\qagentrt.dll,-7  
 Tue Jul 14 04:49:01 2009  
 Z,Netlogon,@%SystemRoot%\System32\netlogon.dll;-102,%systemroot%\system32\lsass.exe,  
 Share\_Process,Manual,LocalSystem,@%SystemRoot%\System32\netlogon.dll,-103  
 Tue Jul 14 04:49:01 2009  
 Z,Netman,@%SystemRoot%\system32\netman.dll;-109,%SystemRoot%\System32\svchost.exe -k  
 LocalSystemNetworkRestricted,Share\_Process,Manual,LocalSystem,@%SystemRoot%\system32  
 \netman.dll,-110  
 Tue Jul 14 04:49:01 2009 Z,Netman\Parameters,,%SystemRoot%\System32\netman.dll,,,,  
 Tue Jul 14 04:49:01 2009  
 Z,netprofm,@%SystemRoot%\system32\netprofm.dll;-202,%SystemRoot%\System32\svchost.exe  
 e -k LocalService,Share\_Process,Manual,NT  
 AUTHORITY\LocalService,@%SystemRoot%\system32\netprofm.dll,-203

## SYSTEM OUTPUT

```

Tue Jul 14 04:49:01 2009
Z,netprofm\Parameters,,,%SystemRoot%\System32\netprofm.dll,,,,
Tue Jul 14 04:49:01 2009
Z,NlaSvc,@%SystemRoot%\System32\nlasvc.dll;-1,%SystemRoot%\System32\svchost.exe -k
NetworkService,Share_Process,Auto Start,NT
AUTHORITY\NetworkService,@%SystemRoot%\System32\nlasvc.dll,-2
Tue Jul 14 04:49:01 2009
Z,nsi,@%SystemRoot%\system32\nsisvc.dll;-200,%systemroot%\system32\svchost.exe -k
LocalService,Share_Process,Auto Start,NT
Authority\LocalService,@%SystemRoot%\system32\nsisvc.dll,-201
Tue Jul 14 04:49:01 2009 Z,NTDS,,,,,%SystemRoot%\system32\drivers\nsiproxy.sys,-1
Tue Jul 14 04:49:01 2009
Z,p2pimsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8004,%SystemRoot%\System32\svchost.exe
-k LocalServicePeerNet,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\pnrpsvc.dll,-8005
Tue Jul 14 04:49:01 2009
Z,p2psvc,@%SystemRoot%\system32\p2psvc.dll;-8006,%SystemRoot%\System32\svchost.exe
-k LocalServicePeerNet,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\p2psvc.dll,-8007
Tue Jul 14 04:49:01 2009
Z,PcaSvc,@%SystemRoot%\system32\pcasvc.dll;-1,%systemroot%\system32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\pcasvc.dll,-2
Tue Jul 14 04:49:01 2009 Z,PcaSvc\Parameters,,,%SystemRoot%\System32\pcasvc.dll,,,,
Tue Jul 14 04:49:01 2009 Z,PerfDisk,,,,,Intel Security PEF Service
Tue Jul 14 04:49:01 2009
Z,PerfHost,@%systemroot%\syswow64\perfhost.exe;-2,%SystemRoot%\SysWow64\perfhost.exe
,Own_Process,Manual,NT AUTHORITY\LocalService,@%systemroot%\SysWow64\perfhost.exe,-1
Tue Jul 14 04:49:01 2009 Z,PerfNet,,,,,%systemroot%\SysWow64\perfhost.exe,-1
Tue Jul 14 04:49:01 2009 Z,PerfOS,,,,,%systemroot%\SysWow64\perfhost.exe,-1
Tue Jul 14 04:49:01 2009 Z,PerfProc,,,,,%systemroot%\SysWow64\perfhost.exe,-1
Tue Jul 14 04:49:01 2009
Z,pla,@%systemroot%\system32\pla.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\pla.dll,-501
Tue Jul 14 04:49:01 2009 Z,pla\Parameters,,,%systemroot%\system32\pla.dll,,,,
Tue Jul 14 04:49:01 2009
Z,PlugPlay,@%SystemRoot%\system32\umpnpmgr.dll;-100,%SystemRoot%\system32\svchost.exe
-k DcomLaunch,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\umpnpmgr.dll,-101
Tue Jul 14 04:49:01 2009
Z,PNRPAutoReg,@%SystemRoot%\system32\pnrpauto.dll;-8002,%SystemRoot%\System32\svchos
t.exe -k LocalServicePeerNet,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\pnrpauto.dll,-8003
Tue Jul 14 04:49:01 2009
Z,PNRPSvc,@%SystemRoot%\system32\pnrpsvc.dll;-8000,%SystemRoot%\System32\svchost.exe
-k LocalServicePeerNet,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\pnrpsvc.dll,-8001

```



## SYSTEM OUTPUT

Tue Jul 14 04:49:01 2009 Z,PNRPSvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,  
 Tue Jul 14 04:49:01 2009  
 Z,PolicyAgent,@%SystemRoot%\System32\polstore.dll;-5010,%SystemRoot%\system32\svchos  
 t.exe -k NetworkServiceNetworkRestricted,Share\_Process,Manual,NT  
 Authority\NetworkService,@%SystemRoot%\system32\polstore.dll,-5011  
 Tue Jul 14 04:49:01 2009  
 Z,PolicyAgent\Parameters,,%SystemRoot%\System32\ipsecsvc.dll,,,  
 Tue Jul 14 04:49:01 2009 Z,PortProxy,,,,,@%SystemRoot%\system32\polstore.dll,-5011  
 Tue Jul 14 04:49:01 2009  
 Z,Power,@%SystemRoot%\system32\umpo.dll;-100,%SystemRoot%\system32\svchost.exe -k  
 DcomLaunch,Share\_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\umpo.dll,-101  
 Tue Jul 14 04:49:01 2009 Z,Power\Parameters,,%SystemRoot%\system32\umpo.dll,,,  
 Tue Jul 14 04:49:01 2009  
 Z,ProfSvc,@%systemroot%\system32\profsvc.dll;-300,%systemroot%\system32\svchost.exe  
 -k netsvcs,Share\_Process,Auto  
 Start,LocalSystem,@%systemroot%\system32\profsvc.dll,-301  
 Tue Jul 14 04:49:01 2009  
 Z,ProtectedStorage,@%systemroot%\system32\psbase.dll;-300,%SystemRoot%\system32\lsas  
 s.exe,Share\_Process,Manual,LocalSystem,@%systemroot%\system32\psbase.dll,-301  
 Tue Jul 14 04:49:01 2009  
 Z,QWAVE,@%SystemRoot%\system32\qwave.dll;-1,%windir%\system32\svchost.exe -k  
 LocalServiceAndNoImpersonation,Share\_Process,Manual,NT  
 AUTHORITY\LocalService,@%SystemRoot%\system32\qwave.dll,-2  
 Tue Jul 14 04:49:01 2009 Z,QWAVE\Parameters,,%windir%\system32\qwave.dll,,,  
 Tue Jul 14 04:49:01 2009  
 Z,QWAVEdrv,@%SystemRoot%\system32\drivers\qwavedrv.sys;-1,\SystemRoot\system32\drive  
 rs\qwavedrv.sys,Kernel driver,Manual,,@%SystemRoot%\system32\drivers\qwavedrv.sys,-2  
 Tue Jul 14 04:49:01 2009 Z,RasAcid,Remote Access Auto Connection  
 Driver,System32\DRIVERS\rasacd.sys,Kernel driver,Manual,,Remote Access Auto  
 Connection Driver  
 Tue Jul 14 04:49:01 2009 Z,RDPDD,,,,,@%systemroot%\system32\DRIVERS\RDPCDD.sys,-101  
 Tue Jul 14 04:49:01 2009  
 Z,RDPNP,@%systemroot%\system32\drprov.dll;-100,,,,@%systemroot%\system32\drprov.dll  
 ,-101  
 Tue Jul 14 04:49:01 2009 Z,RDPWD,RDP Winstation Driver,,Kernel  
 driver,Manual,,@%systemroot%\system32\drivers\RdpRefMp.sys,-100  
 Tue Jul 14 04:49:01 2009  
 Z,RemoteRegistry,@regsvc.dll;-1,%SystemRoot%\system32\svchost.exe -k  
 regsvc,Share\_Process,Manual,NT AUTHORITY\LocalService,@regsvc.dll,-2  
 Tue Jul 14 04:49:01 2009  
 Z,RemoteRegistry\Parameters,,%SystemRoot%\system32\regsvc.dll,,,  
 Tue Jul 14 04:49:01 2009  
 Z,RpcLocator,@%systemroot%\system32\Locator.exe;-2,%SystemRoot%\system32\locator.exe  
 ,Own\_Process,Manual,NT  
 AUTHORITY\NetworkService,@%systemroot%\system32\Locator.exe,-3  
 Tue Jul 14 04:49:01 2009 Z,RpcSs,@oleres.dll;-5010,%SystemRoot%\system32\svchost.exe  
 -k rpcss,Share\_Process,Auto Start,NT AUTHORITY\NetworkService,@oleres.dll,-5011  
 Tue Jul 14 04:49:01 2009

## SYSTEM OUTPUT

```

Z,SCardSvr\Parameters,,%SystemRoot%\System32\SCardSvr.dll,,,,
Tue Jul 14 04:49:01 2009
Z,Schedule,@%SystemRoot%\system32\schedsvc.dll;-100,%systemroot%\system32\svchost.exe -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\system32\schedsvc.dll,-101
Tue Jul 14 04:49:01 2009
Z,Schedule\Parameters,,%systemroot%\system32\schedsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SCPolicySvc,@%SystemRoot%\System32\certprop.dll;-13,%SystemRoot%\system32\svchost.exe -k
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\System32\certprop.dll,-14
Tue Jul 14 04:49:01 2009
Z,SCPolicySvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SDRSVC,@%SystemRoot%\system32\sdrsvc.dll;-107,%SystemRoot%\system32\svchost.exe -k
SDRSVC,Own_Process,Manual,localSystem,@%SystemRoot%\system32\sdrsvc.dll,-102
Tue Jul 14 04:49:01 2009
Z,seclogon,@%SystemRoot%\system32\seclogon.dll;-7001,%windir%\system32\svchost.exe -k
netsvcs,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\seclogon.dll,-7000
Tue Jul 14 04:49:01 2009 Z,seclogon\Parameters,,%windir%\system32\seclogon.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SENS,@%SystemRoot%\system32\Sens.dll;-200,%SystemRoot%\system32\svchost.exe -k
netsvcs,Share_Process,Auto Start,LocalSystem,@%SystemRoot%\system32\Sens.dll,-201
Tue Jul 14 04:49:01 2009 Z,SENS\Parameters,,%SystemRoot%\System32\sens.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SessionEnv\Parameters,,%SystemRoot%\system32\sessenv.dll,,,,
Tue Jul 14 04:49:01 2009
Z,ShellHWDetection,@%SystemRoot%\System32\shsvcs.dll;-12288,%SystemRoot%\System32\svchost.exe -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\System32\shsvcs.dll,-12289
Tue Jul 14 04:49:01 2009
Z,ShellHWDetection\Parameters,,%SystemRoot%\System32\shsvcs.dll,,,,
Tue Jul 14 04:49:01 2009
Z,SNMPTRAP,@%SystemRoot%\system32\snmptrap.exe;-3,%SystemRoot%\System32\snmptrap.exe,Own_Process,Manual,NT AUTHORITY\LocalService,@%SystemRoot%\system32\snmptrap.exe,-4
Tue Jul 14 04:49:01 2009
Z,Spooler,@%systemroot%\system32\spoolsv.exe;-1,%SystemRoot%\System32\spoolsv.exe,Own_Process,Auto Start,LocalSystem,@%systemroot%\system32\spoolsv.exe,-2
Tue Jul 14 04:49:01 2009
Z,sppsvc,@%SystemRoot%\system32\sppsvc.exe;-101,%SystemRoot%\system32\sppsvc.exe,Own_Process,Auto Start,NT
AUTHORITY\NetworkService,@%SystemRoot%\system32\sppsvc.exe,-100
Tue Jul 14 04:49:01 2009
Z,sppuotify,@%SystemRoot%\system32\sppuotify.dll;-103,%SystemRoot%\system32\svchost.exe -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\sppuotify.dll,-102
Tue Jul 14 04:49:01 2009

```

## SYSTEM OUTPUT

Z,sppuinotify\Parameters,,,%SystemRoot%\system32\sppuinotify.dll,,,,,  
Tue Jul 14 04:49:01 2009  
Z,SSDPSRV,@%systemroot%\system32\ssdpsrv.dll;-100,%SystemRoot%\system32\svchost.exe  
-k LocalServiceAndNoImpersonation,Share\_Process,Manual,NT  
AUTHORITY\LocalService,@%systemroot%\system32\ssdpsrv.dll,-101  
Tue Jul 14 04:49:01 2009 Z,SSDPSRV\Parameters,,,%SystemRoot%\System32\ssdpsrv.dll,,,,,  
Tue Jul 14 04:49:01 2009  
Z,SstpSvc,@%SystemRoot%\system32\sstpsvc.dll;-200,%SystemRoot%\system32\svchost.exe  
-k LocalService,Share\_Process,Manual,NT  
Authority\LocalService,@%SystemRoot%\system32\sstpsvc.dll,-201  
Tue Jul 14 04:49:01 2009 Z,stisvc\Parameters,,,%SystemRoot%\System32\wiaservc.dll,,,,,  
Tue Jul 14 04:49:01 2009  
Z,swprv,@%SystemRoot%\System32\swprv.dll;-103,%SystemRoot%\System32\svchost.exe -k  
swprv,Own\_Process,Manual,LocalSystem,@%SystemRoot%\System32\swprv.dll,-102  
Tue Jul 14 04:49:01 2009 Z,swprv\Parameters,,,%Systemroot%\System32\swprv.dll,,,,,  
Tue Jul 14 04:49:01 2009 Z,SysMain\Parameters,,,%systemroot%\system32\sysmain.dll,,,,,  
Tue Jul 14 04:49:01 2009  
Z,TabletInputService,@%SystemRoot%\system32\TabSvc.dll;-100,%SystemRoot%\System32\sv  
chost.exe -k  
LocalSystemNetworkRestricted,Share\_Process,Manual,LocalSystem,@%SystemRoot%\system32  
\TabSvc.dll,-101  
Tue Jul 14 04:49:01 2009  
Z,TabletInputService\Parameters,,,%SystemRoot%\System32\TabSvc.dll,,,,,  
Tue Jul 14 04:49:01 2009  
Z,TapiSrv,@%SystemRoot%\system32\tapisrv.dll;-10100,%SystemRoot%\System32\svchost.ex  
e -k NetworkService,Share\_Process,Manual,NT  
AUTHORITY\NetworkService,@%SystemRoot%\system32\tapisrv.dll,-10101  
Tue Jul 14 04:49:01 2009 Z,TapiSrv\Parameters,,,%SystemRoot%\System32\tapisrv.dll,,,,,  
Tue Jul 14 04:49:01 2009 Z,TCPIP6TUNNEL,,,,,Microsoft IPv6 Protocol Driver  
Tue Jul 14 04:49:01 2009 Z,TCPIPTUNNEL,,,,,Provides compatibility for legacy  
applications which interact with TCP/IP through the registry. If this service is  
stopped, certain applications may have impaired functionality.  
Tue Jul 14 04:49:01 2009 Z,TDPIPE,TDPIPE,system32\drivers\tdpipe.sys,Kernel  
driver,Manual,,Provides compatibility for legacy applications which interact with  
TCP/IP through the registry. If this service is stopped, certain applications may  
have impaired functionality.  
Tue Jul 14 04:49:01 2009 Z,TDTCP,TDTCP,system32\drivers\tdtcp.sys,Kernel  
driver,Manual,,Provides compatibility for legacy applications which interact with  
TCP/IP through the registry. If this service is stopped, certain applications may  
have impaired functionality.  
Tue Jul 14 04:49:01 2009  
Z,TermService,@%SystemRoot%\System32\termsrv.dll;-268,%SystemRoot%\System32\svchost.  
exe -k NetworkService,Share\_Process,Manual,NT  
Authority\NetworkService,@%SystemRoot%\System32\termsrv.dll,-267  
Tue Jul 14 04:49:01 2009  
Z,TermService\Parameters,,,%SystemRoot%\System32\termsrv.dll,,,,,  
Tue Jul 14 04:49:01 2009  
Z,Themes,@%SystemRoot%\System32\themeservice.dll;-8192,%SystemRoot%\System32\svchost

## SYSTEM OUTPUT

```
.exe -k netsvcs,Share_Process,Auto
Start,LocalSystem,@%SystemRoot%\System32\themeservice.dll,-8193
Tue Jul 14 04:49:01 2009
Z,Themes\Parameters,,%SystemRoot%\system32\themeservice.dll,,,
Tue Jul 14 04:49:01 2009
Z,THREADORDER,@%systemroot%\system32\mmcscs.dll;-102,%SystemRoot%\system32\svchost.exe
-k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\mmcscs.dll,-103
Tue Jul 14 04:49:01 2009
Z,TSDDD,,,,,@%SystemRoot%\servicing\TrustedInstaller.exe,-101
Tue Jul 14 04:49:01 2009
Z,tssecsrv,@%SystemRoot%\System32\DRIVERS\tssecsrv.sys;-101,System32\DRIVERS\tssecsrv.sys,Kernel driver,Manual,,@%SystemRoot%\System32\DRIVERS\tssecsrv.sys,-102
Tue Jul 14 04:49:01 2009 Z,UGatherer,,,,,Reads/Writes UDF 1.02,1.5,2.0x,2.5 disc formats, usually found on C/DVD discs. (Core) (All pieces)
Tue Jul 14 04:49:01 2009 Z,UGTHRSVC,,,,,Reads/Writes UDF 1.02,1.5,2.0x,2.5 disc formats, usually found on C/DVD discs. (Core) (All pieces)
Tue Jul 14 04:49:01 2009
Z,UI0Detect,@%SystemRoot%\system32\ui0detect.exe;-101,%SystemRoot%\system32\UI0Detect.exe,Own_Process,Manual,LocalSystem,@%SystemRoot%\system32\ui0detect.exe,-102
Tue Jul 14 04:49:01 2009
Z,upnphost,@%systemroot%\system32\upnphost.dll;-213,%SystemRoot%\system32\svchost.exe
-k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%systemroot%\system32\upnphost.dll,-214
Tue Jul 14 04:49:01 2009
Z,upnphost\Parameters,,%SystemRoot%\System32\upnphost.dll,,,
Tue Jul 14 04:49:01 2009
Z,UxSms,@%SystemRoot%\system32\dwm.exe;-2000,%SystemRoot%\System32\svchost.exe -k
LocalSystemNetworkRestricted,Share_Process,Auto
Start,localSystem,@%SystemRoot%\system32\dwm.exe,-2001
Tue Jul 14 04:49:01 2009 Z,UxSms\Parameters,,%SystemRoot%\System32\uxsms.dll,,,
Tue Jul 14 04:49:01 2009
Z,VaultSvc,@%SystemRoot%\system32\vaultsvc.dll;-1003,%SystemRoot%\system32\lsass.exe
,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32\vaultsvc.dll,-1004
Tue Jul 14 04:49:01 2009
Z,vds,@%SystemRoot%\system32\vds.exe;-100,%SystemRoot%\System32\vds.exe,Own_Process,Manual,LocalSystem,@%SystemRoot%\system32\vds.exe,-112
Tue Jul 14 04:49:01 2009
Z,VSS,@%systemroot%\system32\vssvc.exe;-102,%systemroot%\system32\vssvc.exe,Own_Process,Manual,LocalSystem,@%systemroot%\system32\vssvc.exe,-101
Tue Jul 14 04:49:01 2009 Z,W3SVC,,,,,@%SystemRoot%\system32\w32time.dll,-201
Tue Jul 14 04:49:01 2009
Z,wbengine,@%systemroot%\system32\wbengine.exe;-104,"%systemroot%\system32\wbengine.exe",Own_Process,Manual,localSystem,@%systemroot%\system32\wbengine.exe,-105
Tue Jul 14 04:49:01 2009
Z,WbioSrv\Parameters,,%SystemRoot%\System32\wbiosrv.dll,,,
Tue Jul 14 04:49:01 2009
Z,wcncsvc,@%SystemRoot%\system32\wcncsvc.dll;-3,%SystemRoot%\System32\svchost.exe -k
```

## SYSTEM OUTPUT

```

LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\wcncsvc.dll,-4
Tue Jul 14 04:49:01 2009 Z,wcncsvc\Parameters,,%SystemRoot%\System32\wcncsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,WcsPlugInService,@%SystemRoot%\system32\WcsPlugInService.dll;-200,%SystemRoot%\sys
tem32\svchost.exe -k wcscsvc,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\WcsPlugInService.dll,-201
Tue Jul 14 04:49:01 2009
Z,WcsPlugInService\Parameters,,%SystemRoot%\System32\WcsPlugInService.dll,,,,
Tue Jul 14 04:49:01 2009
Z,Wecsvc,@%SystemRoot%\system32\wecsvc.dll;-200,%SystemRoot%\system32\svchost.exe -k
NetworkService,Share_Process,Manual,NT
AUTHORITY\NetworkService,@%SystemRoot%\system32\wecsvc.dll,-201
Tue Jul 14 04:49:01 2009 Z,Wecsvc\Parameters,,%SystemRoot%\system32\wecsvc.dll,,,
Tue Jul 14 04:49:01 2009
Z,wercplsupport,@%SystemRoot%\System32\wercplsupport.dll;-101,%SystemRoot%\System32\
svchost.exe -k
netsvcs,Share_Process,Manual,localSystem,@%SystemRoot%\System32\wercplsupport.dll,-1
00
Tue Jul 14 04:49:01 2009
Z,wercplsupport\Parameters,,%SystemRoot%\System32\wercplsupport.dll,,,,
Tue Jul 14 04:49:01 2009
Z,WerSvc,@%SystemRoot%\System32\wersvc.dll;-100,%SystemRoot%\System32\svchost.exe -k
WerSvcGroup,Share_Process,Manual,localSystem,@%SystemRoot%\System32\wersvc.dll,-101
Tue Jul 14 04:49:01 2009 Z,WinDefend\Parameters,,%ProgramFiles%\Windows
Defender\mpsvc.dll,,,,
Tue Jul 14 04:49:01 2009
Z,WinHttpAutoProxySvc,@%SystemRoot%\system32\winhttp.dll;-100,%SystemRoot%\system32\
svchost.exe -k LocalService,Share_Process,Manual,NT
AUTHORITY\LocalService,@%SystemRoot%\system32\winhttp.dll,-101
Tue Jul 14 04:49:01 2009
Z,WinRM,@%Systemroot%\system32\wsmsvc.dll;-101,%SystemRoot%\System32\svchost.exe -k
NetworkService,Share_Process,Manual,NT
AUTHORITY\NetworkService,@%Systemroot%\system32\wsmsvc.dll,-102
Tue Jul 14 04:49:01 2009 Z,WinRM\Parameters,,%SystemRoot%\system32\WsmSvc.dll,,,,
Tue Jul 14 04:49:01 2009 Z,WinSock2,,,,,@%Systemroot%\system32\wsmsvc.dll,-102
Tue Jul 14 04:49:01 2009
Z,WPCSvc,@%SystemRoot%\system32\wpcsvc.dll;-100,%SystemRoot%\system32\svchost.exe -k
LocalServiceNetworkRestricted,Share_Process,Manual,NT
Authority\LocalService,@%SystemRoot%\system32\wpcsvc.dll,-101
Tue Jul 14 04:49:01 2009
Z,WPDBusEnum,@%SystemRoot%\system32\wpdbusenum.dll;-100,%SystemRoot%\system32\svchos
t.exe -k
LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem,@%SystemRoot%\system32
\wpdbusenum.dll,-101
Tue Jul 14 04:49:01 2009
Z,WPDBusEnum\Parameters,,%SystemRoot%\system32\wpdbusenum.dll,,,
Tue Jul 14 04:49:01 2009

```

## SYSTEM OUTPUT

Z,wscsvc,@%SystemRoot%\System32\wscsvc.dll;-200,%SystemRoot%\System32\svchost.exe -k  
 LocalServiceNetworkRestricted,Share\_Process,Auto Start,NT  
 AUTHORITY\LocalService,@%SystemRoot%\System32\wscsvc.dll,-201  
 Tue Jul 14 04:49:01 2009 Z,wscsvc\Parameters,,%SystemRoot%\System32\wscsvc.dll,,,,  
 Tue Jul 14 04:49:01 2009  
 Z,WSearchIdxPi,,,,,@%systemroot%\system32\SearchIndexer.exe,-104  
 Tue Jul 14 04:49:01 2009  
 Z,wuauerv\Parameters,,%systemroot%\system32\wuaueng.dll,,,,  
 Tue Jul 14 04:49:01 2009 Z,wudfsvc\Parameters,,%SystemRoot%\System32\WUDFSvc.dll,,,,  
 Tue Jul 14 04:49:01 2009  
 Z,WwanSvc,@%SystemRoot%\System32\wwansvc.dll;-257,%SystemRoot%\system32\svchost.exe  
 -k LocalServiceNoNetwork,Share\_Process,Manual,NT  
 Authority\LocalService,@%SystemRoot%\System32\wwansvc.dll,-258  
 Tue Jul 14 04:49:01 2009 Z,WwanSvc\Parameters,,%SystemRoot%\System32\wwansvc.dll,,,,  
 Tue Jul 14 04:49:01 2009 Z,xmlprov,,,,,@%SystemRoot%\System32\wwansvc.dll,-258  
 Tue Jul 14 02:34:41 2009  
 Z,DcomLaunch\Parameters,,%SystemRoot%\system32\rpcss.dll,,,,  
 Tue Jul 14 02:34:41 2009 Z,RpcSs\Parameters,,%SystemRoot%\system32\rpcss.dll,,,,  
 -----  
 Wed Apr 20 02:39:31  
 2016Z,AsyncMac,@%systemroot%\system32\rascfg.dll;-32000,system32\DRIVERS\asyncmac.sys,  
 Kernel driver,Manual,  
 Wed Apr 20 02:39:13 2016Z,mfeaack,McAfee Inc.  
 mfeaack,system32\drivers\mfeaack.sys,Kernel driver,Manual,  
 Wed Apr 20 02:39:13 2016Z,mfencbdc,McAfee Inc.  
 mfencbdc,system32\DRIVERS\mfencbdc.sys,Kernel driver,Manual,  
 Wed Apr 20 02:37:21 2016Z,mfefirek,McAfee Inc.  
 mfefirek,system32\drivers\mfefirek.sys,Kernel driver,Manual,  
 Wed Apr 20 02:37:20 2016Z,cfwids,McAfee Inc.  
 cfwids,system32\drivers\cfwids.sys,Kernel driver,Manual,  
 Wed Apr 20 02:37:04  
 2016Z,LanmanServer\Parameters,,%SystemRoot%\system32\srvsvc.dll,,  
 Wed Apr 20 02:37:01 2016Z,mfemms,McAfee Service Controller,"C:\Program Files\Common  
 Files\McAfee\SystemCore\mfemms.exe",Own\_Process,Auto Start,LocalSystem  
 Wed Apr 20 02:36:56 2016Z,vwifimp,Microsoft Virtual WiFi Miniport  
 Service,system32\DRIVERS\vwifimp.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:49 2016Z,BrSerIb,Brother Serial Interface  
 Driver(WDM),system32\DRIVERS\BrSerIb.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:49 2016Z,BrUsbSIb,Brother Serial USB  
 Driver(WDM),system32\DRIVERS\BrUsbSIb.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:49 2016Z,BthEnum,Bluetooth Enumerator  
 Service,system32\DRIVERS\BthEnum.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:49 2016Z,BthPan,Bluetooth Device (Personal Area  
 Network),system32\DRIVERS\bthpan.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:49 2016Z,monitor,Microsoft Monitor Class Function Driver  
 Service,system32\DRIVERS\monitor.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:49 2016Z,mouhid,Mouse HID Driver,system32\DRIVERS\mouhid.sys,Kernel  
 driver,Manual,

## SYSTEM OUTPUT

Wed Apr 20 02:36:49 2016Z,RFCOMM,Bluetooth Device (RFCOMM Protocol  
 TDI),system32\DRIVERS\rfcomm.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:49 2016Z,usbprint,Microsoft USB PRINTER  
 Class,system32\DRIVERS\usbprint.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:49 2016Z,usbscan,USB Scanner  
 Driver,system32\DRIVERS\usbscan.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:48 2016Z,BTHUSB,Bluetooth Radio USB  
 Driver,system32\DRIVERS\BTHUSB.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:48 2016Z,HidUsb,Microsoft HID Class  
 Driver,system32\DRIVERS\hidusb.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:48 2016Z,kbdhid,Keyboard HID  
 Driver,system32\DRIVERS\kbdhid.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:48  
 2016Z,scfilter,@%SystemRoot%\System32\drivers\scfilter.sys;-11,system32\DRIVERS\scfi  
 lter.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:48 2016Z,WinUSB,WinUSB Service,system32\DRIVERS\WinUSB.sys,Kernel  
 driver,Manual,  
 Wed Apr 20 02:36:48 2016Z,WUDFRd,,system32\DRIVERS\WUDFRd.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:46 2016Z,SPUVCbv,SPUVCb Driver  
 Service,system32\DRIVERS\SPUVCbv\_x64.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:44 2016Z,usbccgp,Microsoft USB Generic Parent  
 Driver,system32\DRIVERS\usbccgp.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:42 2016Z,mfeavfk,McAfee Inc.  
 mfeavfk,system32\drivers\mfeavfk.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:41 2016Z,AgereSoftModem,Agere Systems Soft  
 Modem,system32\DRIVERS\agrsm64.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:41 2016Z,HdAudAddService,Microsoft 1.1 UAA Function Driver for High  
 Definition Audio Service,system32\drivers\HdAudio.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:41 2016Z,IntcDAud,Intel(R) Display  
 Audio,system32\DRIVERS\IntcDAud.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:41 2016Z,ksthunk,Kernel Streaming  
 Thunks,\SystemRoot\system32\drivers\ksthunk.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:41 2016Z,Modem,,system32\drivers\modem.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:41 2016Z,nusb3hub,Renesas Electronics USB 3.0 Hub  
 Driver,\SystemRoot\system32\drivers\nusb3hub.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:41 2016Z,Parport,Parallel port  
 driver,\SystemRoot\system32\drivers\parport.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:41 2016Z,usbhub,Microsoft USB Standard Hub  
 Driver,system32\DRIVERS\usbhub.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:38 2016Z,mssmbios,Microsoft System Management BIOS  
 Driver,\SystemRoot\system32\drivers\mssmbios.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:34 2016Z,cdrom,CD-ROM Driver,system32\DRIVERS\cdrom.sys,Kernel  
 driver,Manual,  
 Wed Apr 20 02:36:34 2016Z,Disk,Disk Driver,system32\drivers\disk.sys,Kernel  
 driver,Manual,  
 Wed Apr 20 02:36:34 2016Z,hpdskflt,HP Filter,system32\drivers\hpdskflt.sys,Kernel  
 driver,Manual,  
 Wed Apr 20 02:36:34 2016Z,rdyboost,ReadyBoost,system32\drivers\rdyboost.sys,Kernel

## SYSTEM OUTPUT

```

driver,Boot Start,
Wed Apr 20 02:36:33 2016Z,1394ohci,1394 OHCI Compliant Host
Controller,\SystemRoot\system32\drivers\1394ohci.sys,Kernel driver,Manual,
Wed Apr 20 02:36:33 2016Z,Accelerometer,HP Mobile Data Protection
Sensor,\SystemRoot\system32\drivers\Accelerometer.sys,Kernel driver,Manual,
Wed Apr 20 02:36:33 2016Z,ACPI,Microsoft ACPI
Driver,system32\drivers\ACPI.sys,Kernel driver,Boot Start,
Wed Apr 20 02:36:33
2016Z,AFD,@%systemroot%\system32\drivers\afd.sys;-1000,\SystemRoot\system32\drivers\
afd.sys,Kernel driver,System Start,
Wed Apr 20 02:36:33 2016Z,amdkmdag,,system32\DRIVERS\atikmdag.sys,Kernel
driver,Manual,
Wed Apr 20 02:36:33 2016Z,amdkmpfd,AMD PCI Root Bus Lower
Filter,system32\drivers\amdkmpfd.sys,Kernel driver,Boot Start,
Wed Apr 20 02:36:33 2016Z,atapi,IDE Channel,system32\drivers\atapi.sys,Kernel
driver,Boot Start,
Wed Apr 20 02:36:33 2016Z,Beep,Beep,,Kernel driver,System Start,
Wed Apr 20 02:36:33 2016Z,blbdrive,,\SystemRoot\system32\drivers\blbdrive.sys,Kernel
driver,System Start,
Wed Apr 20 02:36:33
2016Z,browser,@%systemroot%\system32\browser.dll;-102,system32\DRIVERS\browser.sys,File
system driver,Manual,
Wed Apr 20 02:36:33 2016Z,cdfs,CD/DVD File System
Reader,system32\DRIVERS\cdfs.sys,File system driver,Disabled,
Wed Apr 20 02:36:33
2016Z,CLFS,@%SystemRoot%\system32\clfs.sys;-100,system32\CLFS.sys,Kernel driver,Boot
Start,
Wed Apr 20 02:36:33 2016Z,CmBatt,Microsoft ACPI Control Method Battery
Driver,\SystemRoot\system32\drivers\CmBatt.sys,Kernel driver,Manual,
Wed Apr 20 02:36:33 2016Z,CNG,,System32\Drivers\cng.sys,Kernel driver,Boot Start,
Wed Apr 20 02:36:33 2016Z,Compbatt,Microsoft Composite Battery
Driver,system32\drivers\compbatt.sys,Kernel driver,Boot Start,
Wed Apr 20 02:36:33 2016Z,CompositeBus,Composite Bus Enumerator
Driver,\SystemRoot\system32\drivers\CompositeBus.sys,Kernel driver,Manual,
Wed Apr 20 02:36:33
2016Z,CSC,@%systemroot%\system32\cscsvc.dll;-202,system32\drivers\csc.sys,Kernel
driver,System Start,
Wed Apr 20 02:36:33
2016Z,DfsC,@%systemroot%\system32\drivers\dfsc.sys;-101,system32\Drivers\dfsc.sys,File
system driver,System Start,
Wed Apr 20 02:36:33
2016Z,discache,@%systemroot%\system32\drivers\discache.sys;-102,system32\drivers\dis
cache.sys,Kernel driver,System Start,
Wed Apr 20 02:36:33 2016Z,DXGKrnl,LDDM Graphics
Subsystem,\SystemRoot\System32\drivers\dxgkrnl.sys,Kernel driver,Manual,
Wed Apr 20 02:36:33 2016Z,e1cexpress,Intel(R) PRO/1000 PCI Express Network
Connection Driver C,system32\DRIVERS\e1c62x64.sys,Kernel driver,Manual,
Wed Apr 20 02:36:33 2016Z,exfat,exFAT File System Driver,,File system driver,Manual,

```



## SYSTEM OUTPUT

Wed Apr 20 02:36:33 2016Z, fastfat, FAT12/16/32 File System Driver,, File system driver, Manual,

Wed Apr 20 02:36:33 2016Z, FileInfo, @%SystemRoot%\system32\drivers\fileinfo.sys; -100, system32\drivers\fileinfo.sys, File system driver, Boot Start,

Wed Apr 20 02:36:33 2016Z, FltMgr, @%SystemRoot%\system32\drivers\fltmg.sys; -10001, system32\drivers\fltmg.sys, File system driver, Boot Start,

Wed Apr 20 02:36:33 2016Z, Fs\_Rec,,, 8, Boot Start,

Wed Apr 20 02:36:33 2016Z, fvevol, @%SystemRoot%\system32\drivers\fvevol.sys; -100, System32\DRIVERS\fvevol.sys, Kernel driver, Boot Start,

Wed Apr 20 02:36:33 2016Z, HDAudBus, Microsoft UAA Bus Driver for High Definition Audio, \SystemRoot\system32\drivers\HDAudBus.sys, Kernel driver, Manual,

Wed Apr 20 02:36:33 2016Z, HTTP, @%SystemRoot%\system32\drivers\http.sys; -1, system32\drivers\HTTP.sys, Kernel driver, Manual,

Wed Apr 20 02:36:33 2016Z, hwpolicy, @%systemroot%\system32\drivers\hwpolicy.sys; -101, System32\drivers\hwpolicy.sys, Kernel driver, Boot Start,

Wed Apr 20 02:36:33 2016Z, i8042prt, i8042 Keyboard and PS/2 Mouse Port Driver, \SystemRoot\system32\drivers\i8042prt.sys, Kernel driver, Manual,

Wed Apr 20 02:36:33 2016Z, igfx,,, system32\DRIVERS\igdkmd64.sys, Kernel driver, Manual,

Wed Apr 20 02:36:33 2016Z, intelppm, Intel Processor Driver, system32\DRIVERS\intelppm.sys, Kernel driver, Manual,

Wed Apr 20 02:36:33 2016Z, JMCR,,, system32\DRIVERS\jmcr.sys, Kernel driver, Manual,

Wed Apr 20 02:36:33 2016Z, kbdclass, Keyboard Class Driver, system32\DRIVERS\kbdclass.sys, Kernel driver, Manual,

Wed Apr 20 02:36:33 2016Z, KSecDD,,, System32\Drivers\ksecdd.sys, Kernel driver, Boot Start,

Wed Apr 20 02:36:33 2016Z, KSecPkg,,, System32\Drivers\ksecpkg.sys, Kernel driver, Boot Start,

Wed Apr 20 02:36:33 2016Z, lltdio, Link-Layer Topology Discovery Mapper I/O Driver, system32\DRIVERS\lltdio.sys, Kernel driver, Auto Start,

Wed Apr 20 02:36:33 2016Z, luafv, @%systemroot%\system32\drivers\luafv.sys; -100, \SystemRoot\system32\drivers\luafv.sys, File system driver, Auto Start,

Wed Apr 20 02:36:33 2016Z, MBAMProtector,,, \??\C:\Windows\system32\drivers\mbam.sys, File system driver, Manual,

Wed Apr 20 02:36:33 2016Z, MBAMSwissArmy, MBAMSwissArmy, \??\C:\Windows\system32\drivers\MBAMSwissArmy.sys, File system driver, Manual,

Wed Apr 20 02:36:33 2016Z, MBAMWebAccessControl,,, \??\C:\Windows\system32\drivers\mwac.sys, File system driver, Manual,

Wed Apr 20 02:36:33 2016Z, MEIx64, Intel(R) Management Engine Interface, \SystemRoot\system32\drivers\HECIx64.sys, Kernel driver, Manual,

## SYSTEM OUTPUT

Wed Apr 20 02:36:33 2016Z,mfehdk,McAfee Inc.  
 mfehdk,system32\drivers\mfehdk.sys,Kernel driver,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,mfencrk,McAfee Inc.  
 mfencrk,system32\DRIVERS\mfencrk.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33 2016Z,mfesapsn,McAfee Process Start Notification  
 Service,\??\C:\Program Files (x86)\McAfee\SiteAdvisor\x64\mfesapsn.sys,Kernel  
 driver,Manual,  
 Wed Apr 20 02:36:33 2016Z,mfewfpk,McAfee Inc.  
 mfewfpk,system32\drivers\mfewfpk.sys,Kernel driver,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,mouclass,Mouse Class  
 Driver,system32\DRIVERS\mouclass.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,mountmgr,@%SystemRoot%\system32\drivers\mountmgr.sys;-100,System32\drivers\mou  
 ntmgr.sys,Kernel driver,Boot Start,  
 Wed Apr 20 02:36:33  
 2016Z,mpsdrv,@%SystemRoot%\system32\FirewallAPI.dll;-23092,System32\drivers\mpsdrv.s  
 ys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,mrxsmb,@%systemroot%\system32\wkssvc.dll;-1002,system32\DRIVERS\mrxsmb.sys,File  
 system driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,mrxsmb10,@%systemroot%\system32\wkssvc.dll;-1004,system32\DRIVERS\mrxsmb10.sys  
 ,File system driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,mrxsmb20,@%systemroot%\system32\wkssvc.dll;-1006,system32\DRIVERS\mrxsmb20.sys  
 ,File system driver,Manual,  
 Wed Apr 20 02:36:33 2016Z,msahci,,system32\drivers\msahci.sys,Kernel driver,Boot  
 Start,  
 Wed Apr 20 02:36:33 2016Z,Msfs,,,File system driver,System Start,  
 Wed Apr 20 02:36:33 2016Z,msisadvr,,system32\drivers\msisadvr.sys,Kernel driver,Boot  
 Start,  
 Wed Apr 20 02:36:33  
 2016Z,Mup,@%systemroot%\system32\drivers\mup.sys;-101,System32\Drivers\mup.sys,File  
 system driver,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,NativeWifiP,NativeWiFi  
 Filter,system32\DRIVERS\nwifi.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,NDIS,@%SystemRoot%\system32\drivers\ndis.sys;-200,system32\drivers\ndis.sys,Ke  
 rnel driver,Boot Start,  
 Wed Apr 20 02:36:33  
 2016Z,NdisTapi,@%systemroot%\system32\rascfg.dll;-32001,system32\DRIVERS\ndistapi.sy  
 s,Kernel driver,Manual,  
 Wed Apr 20 02:36:33 2016Z,Ndisuio,NDIS Usermode I/O  
 Protocol,system32\DRIVERS\ndisuio.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,Ndiswan,@%systemroot%\system32\rascfg.dll;-32002,system32\DRIVERS\ndiswan.sys,  
 Kernel driver,Manual,  
 Wed Apr 20 02:36:33 2016Z,NDProxy,NDIS Proxy,,Kernel driver,Manual,

## SYSTEM OUTPUT

Wed Apr 20 02:36:33 2016Z,NetBIOS,NetBIOS  
 Interface,system32\DRIVERS\netbios.sys,File system driver,System Start,  
 Wed Apr 20 02:36:33  
 2016Z,NetBT,@%SystemRoot%\system32\drivers\netbt.sys;-2,System32\DRIVERS\netbt.sys,K  
 ernel driver,System Start,  
 Wed Apr 20 02:36:33 2016Z,NETwNs64,\_\_\_ Intel(R) Wireless WiFi Link 5000 Series  
 Adapter Driver for Windows 7 - 64 Bit,system32\DRIVERS\NETwsw00.sys,Kernel  
 driver,Manual,  
 Wed Apr 20 02:36:33 2016Z,Npfs,,,File system driver,System Start,  
 Wed Apr 20 02:36:33  
 2016Z,nsiproxy,@%SystemRoot%\system32\drivers\nsiproxy.sys;-2,system32\drivers\nsipr  
 oxy.sys,Kernel driver,System Start,  
 Wed Apr 20 02:36:33 2016Z,Ntfs,,,File system driver,Manual,  
 Wed Apr 20 02:36:33 2016Z,Null,,,Kernel driver,System Start,  
 Wed Apr 20 02:36:33 2016Z,nusb3xhc,Renesas Electronics USB 3.0 Host Controller  
 Driver,\SystemRoot\system32\drivers\nusb3xhc.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,partmgr,@%SystemRoot%\system32\drivers\partmgr.sys;-100,System32\drivers\partm  
 gr.sys,Kernel driver,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,pci,PCI Bus Driver,system32\drivers\pci.sys,Kernel  
 driver,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,pcw,Performance Counters for Windows  
 Driver,System32\drivers\pcw.sys,Kernel driver,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,PEAUTH,PEAUTH,system32\drivers\peauth.sys,Kernel  
 driver,Auto Start,  
 Wed Apr 20 02:36:33  
 2016Z,PptpMiniport,@%systemroot%\system32\rascfg.dll;-32006,system32\DRIVERS\raspptp  
 .sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,Psched,@%SystemRoot%\System32\drivers\pacer.sys;-101,system32\DRIVERS\pacer.sy  
 s,Kernel driver,System Start,  
 Wed Apr 20 02:36:33 2016Z,RasAgileVpn,WAN Miniport  
 (IKEv2),system32\DRIVERS\AgileVpn.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,Rasl2tp,@%systemroot%\system32\rascfg.dll;-32005,system32\DRIVERS\rasl2tp.sys,  
 Kernel driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,RasPppoe,@%systemroot%\system32\rascfg.dll;-32007,system32\DRIVERS\rasppoe.sy  
 s,Kernel driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,RasSstp,@%systemroot%\system32\sstpsvc.dll;-202,system32\DRIVERS\rassstp.sys,K  
 ernel driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,rdbss,@%systemroot%\system32\wkssvc.dll;-1000,system32\DRIVERS\rdbss.sys,File  
 system driver,System Start,  
 Wed Apr 20 02:36:33 2016Z,rdpbus,Remote Desktop Device Redirector Bus  
 Driver,\SystemRoot\system32\drivers\rdpbus.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33

## SYSTEM OUTPUT

2016Z,RDPCDD,@%systemroot%\system32\DRIVERS\RDPCDD.sys;-100,System32\DRIVERS\RDPCDD.sys,Kernel driver,System Start,  
 Wed Apr 20 02:36:33  
 2016Z,RDPENCDD,@%systemroot%\system32\drivers\RDPCDD.sys;-101,system32\drivers\rdpencdd.sys,Kernel driver,System Start,  
 Wed Apr 20 02:36:33  
 2016Z,RDPREFMP,@%systemroot%\system32\drivers\RdpRefMp.sys;-101,system32\drivers\rdprefmp.sys,Kernel driver,System Start,  
 Wed Apr 20 02:36:33 2016Z,rsndr,Link-Layer Topology Discovery Responder,system32\DRIVERS\rsndr.sys,Kernel driver,Auto Start,  
 Wed Apr 20 02:36:33 2016Z,secdrv,Security Driver,,Kernel driver,Disabled,  
 Wed Apr 20 02:36:33 2016Z,Serenum,Serenum Filter Driver,system32\DRIVERS\serenum.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33 2016Z,Serial,Serial port driver,system32\DRIVERS\serial.sys,Kernel driver,System Start,  
 Wed Apr 20 02:36:33 2016Z,spldr,Security Processor Loader Driver,,Kernel driver,Boot Start,  
 Wed Apr 20 02:36:33  
 2016Z,srv,@%systemroot%\system32\srvc.dll;-102,System32\DRIVERS\srv.sys,File system driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,srv2,@%systemroot%\system32\srvc.dll;-104,System32\DRIVERS\srv2.sys,File system driver,Manual,  
 Wed Apr 20 02:36:33 2016Z,srvnet,,System32\DRIVERS\srvnet.sys,File system driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,storflt,@%SystemRoot%\system32\vmstorfltres.dll;-1000,system32\drivers\vmstorflt.sys,Kernel driver,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,swenum,Software Bus Driver,\SystemRoot\system32\drivers\swenum.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,Tcpip,@%SystemRoot%\system32\tcpipcfg.dll;-50003,System32\drivers\tcpip.sys,Kernel driver,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,tcpipreg,TCP/IP Registry Compatibility,System32\drivers\tcpipreg.sys,Kernel driver,Auto Start,  
 Wed Apr 20 02:36:33  
 2016Z,tdx,@%SystemRoot%\system32\tcpipcfg.dll;-50004,system32\DRIVERS\tdx.sys,Kernel driver,System Start,  
 Wed Apr 20 02:36:33 2016Z,TermDD,Terminal Device Driver,\SystemRoot\system32\drivers\termdd.sys,Kernel driver,System Start,  
 Wed Apr 20 02:36:33 2016Z,TPM,TPM,system32\drivers\tpm.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33 2016Z,tunnel,Microsoft Tunnel Miniport Adapter Driver,system32\DRIVERS\tunnel.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33 2016Z,udfs,udfs,system32\DRIVERS\udfs.sys,File system driver,Disabled,  
 Wed Apr 20 02:36:33 2016Z,umbus,UMBus Enumerator Driver,\SystemRoot\system32\drivers\umbus.sys,Kernel driver,Manual,  
 Wed Apr 20 02:36:33 2016Z,usbehci,Microsoft USB 2.0 Enhanced Host Controller

## SYSTEM OUTPUT

Miniport Driver, \SystemRoot\system32\drivers\usbhcd.sys, Kernel driver, Manual,  
 Wed Apr 20 02:36:33 2016Z, vdrvroot, Microsoft Virtual Drive Enumerator  
 Driver, system32\drivers\vdrvroot.sys, Kernel driver, Boot Start,  
 Wed Apr 20 02:36:33 2016Z, VgaSave, \SystemRoot\System32\drivers\vga.sys, Kernel  
 driver, System Start,  
 Wed Apr 20 02:36:33 2016Z, volmgr, Volume Manager  
 Driver, system32\drivers\volmgr.sys, Kernel driver, Boot Start,  
 Wed Apr 20 02:36:33  
 2016Z, volmgrx, @%SystemRoot%\system32\drivers\volmgrx.sys; -100, system32\drivers\volmg  
 rx.sys, Kernel driver, Boot Start,  
 Wed Apr 20 02:36:33 2016Z, volsnap, Storage  
 volumes, system32\drivers\volsnap.sys, Kernel driver, Boot Start,  
 Wed Apr 20 02:36:33 2016Z, vwifibus, Virtual WiFi Bus  
 Driver, system32\DRIVERS\vwifibus.sys, Kernel driver, Manual,  
 Wed Apr 20 02:36:33 2016Z, vwififlt, Virtual WiFi Filter  
 Driver, system32\DRIVERS\vwififlt.sys, Kernel driver, System Start,  
 Wed Apr 20 02:36:33  
 2016Z, Wanarpv6, @%systemroot%\system32\rascfg.dll; -32012, system32\DRIVERS\wanarp.sys,  
 Kernel driver, System Start,  
 Wed Apr 20 02:36:33  
 2016Z, Wdf01000, @%SystemRoot%\system32\drivers\Wdf01000.sys; -1000, system32\drivers\Wd  
 f01000.sys, Kernel driver, Boot Start,  
 Wed Apr 20 02:36:33 2016Z, WfpLwf, WFP Lightweight  
 Filter, system32\DRIVERS\wfplwf.sys, Kernel driver, System Start,  
 Wed Apr 20 02:36:33 2016Z, WIMMount, WIMMount, system32\drivers\wimmount.sys, File  
 system driver, Manual,  
 Wed Apr 20 02:36:33 2016Z, WmiAcpi, Microsoft Windows Management Interface for  
 ACPI, \SystemRoot\system32\drivers\wmiaapi.sys, Kernel driver, Manual,  
 Wed Apr 20 02:36:33 2016Z, ws2ifsl, Windows Socket 2.0 Non-IFS Service Provider  
 Support Environment, \SystemRoot\system32\drivers\ws2ifsl.sys, Kernel driver, System  
 Start,  
 Wed Apr 20 02:36:33  
 2016Z, WudfPf, @%SystemRoot%\system32\drivers\Wudfpf.sys; -1000, system32\drivers\WudfPf  
 .sys, Kernel driver, Manual,  
 Tue Apr 19 01:25:12 2016Z, MSK80Service, McAfee Anti-Spam Service, "C:\Program  
 Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"  
 /McCoreSvc, Share\_Process, Auto Start, LocalSystem  
 Tue Apr 19 01:25:10 2016Z, McProxy, McAfee Proxy Service, "C:\Program Files\Common  
 Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc, Share\_Process, Auto  
 Start, LocalSystem  
 Tue Apr 19 01:25:09 2016Z, McNaiAnn, McAfee VirusScan Announcer, "C:\Program  
 Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"  
 /McCoreSvc, Share\_Process, Auto Start, LocalSystem  
 Tue Apr 19 01:25:08 2016Z, McMPFSvc, McAfee Personal Firewall Service, "C:\Program  
 Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"  
 /McCoreSvc, Share\_Process, Auto Start, LocalSystem  
 Tue Apr 19 01:25:06 2016Z, McBootDelayStartSvc, McAfee Boot Delay Start  
 Service, "C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"

## SYSTEM OUTPUT

/McCoreSvc,Share\_Process,Auto Start,LocalSystem  
 Tue Apr 19 01:25:05 2016Z,HomeNetSvc,McAfee Home Network,"C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,Share\_Process,Auto Start,LocalSystem  
 Tue Apr 19 01:25:04 2016Z,McAPExe,McAfee AP Service,"C:\Program Files\McAfee\MSC\McAPExe.exe",Own\_Process,Auto Start,LocalSystem  
 Tue Apr 19 01:25:03 2016Z,mfefire,McAfee Firewall Core Service,"C:\Program Files\Common Files\McAfee\SystemCore\mfefire.exe",Own\_Process,Manual,LocalSystem  
 Tue Apr 19 01:25:00 2016Z,mfevtp,McAfee Validation Trust Protection Service,"C:\Windows\system32\mfevtps.exe",Own\_Process,Manual,LocalSystem  
 Tue Apr 19 01:22:11 2016Z,McAfee SiteAdvisor Service,McAfee SiteAdvisor Service,"C:\Program Files (x86)\McAfee\SiteAdvisor\McSACore.exe",Own\_Process,Auto Start,LocalSystem  
 Tue Apr 19 01:21:52 2016Z,mcpltsvc,McAfee Platform Services,"C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,Share\_Process,Auto Start,LocalSystem  
 Tue Apr 19 01:21:37 2016Z,PEFService,Intel Security PEF Service,"C:\Program Files\Common Files\Intel Security\PEF\CORE\PEFService.exe",Own\_Process,Auto Start,LocalSystem  
 Tue Apr 19 01:21:20 2016Z,mccspsvc,McAfee CSP Service,"C:\Program Files\Common Files\McAfee\CSP\1.8.267.0\McCSPServiceHost.exe",Own\_Process,Auto Start,LocalSystem  
 Sat Apr 16 22:47:57 2016Z,MSPQM,Microsoft Streaming Quality Manager Proxy,system32\drivers\MSPQM.sys,Kernel driver,Manual,  
 Wed Apr 13 11:43:26 2016Z,TrustedInstaller,@%SystemRoot%\servicing\TrustedInstaller.exe;-100,%SystemRoot%\servicing\TrustedInstaller.exe,Own\_Process,Manual,localSystem  
 Wed Apr 13 11:42:56 2016Z,PlugPlay\Parameters,,%SystemRoot%\system32\umpnpgmgr.dll,,,  
 Wed Apr 6 14:20:46 2016Z,USBSTOR,USB Mass Storage Driver,system32\DRIVERS\USBSTOR.SYS,Kernel driver,Manual,  
 Wed Apr 6 00:30:11 2016Z,Winsmgmt\Parameters,,%SystemRoot%\system32\wbem\WMIsvc.dll,,,  
 Sun Mar 27 00:31:42 2016Z,MBAMScheduler,,,"C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamscheduler.exe",Own\_Process,Auto Start,LocalSystem  
 Sun Mar 27 00:31:41 2016Z,MBAMService,,,"C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamservice.exe",Own\_Process,Auto Start,LocalSystem  
 Thu Mar 10 19:38:21 2016Z,Netaapl,Apple Mobile Device Ethernet Service,system32\DRIVERS\netaapl64.sys,Kernel driver,Manual,  
 Thu Mar 10 19:38:21 2016Z,USBAAPL64,Apple Mobile USB Driver,system32\Drivers\usbaapl64.sys,Kernel driver,Manual,  
 Thu Feb 25 02:16:29 2016Z,usbaudio,USB Audio Driver (WDM),system32\drivers\usbaudio.sys,Kernel driver,Manual,  
 Sun Feb 21 00:01:18 2016Z,WinDefend,@%ProgramFiles%\Windows Defender\MsMpRes.dll;-103,%SystemRoot%\System32\svchost.exe -k secsvcs,Share\_Process,Manual,LocalSystem  
 Sun Feb 14 15:57:33 2016Z,drmkaud,Microsoft Trusted Audio Drivers,\SystemRoot\system32\drivers\drmkaud.sys,Kernel driver,Manual,  
 Sun Feb 14 15:57:33 2016Z,MSKSSRV,Microsoft Streaming Service Proxy,system32\drivers\MSKSSRV.sys,Kernel driver,Manual,

## SYSTEM OUTPUT

Sun Feb 14 15:57:33 2016Z,MSPCLOCK,Microsoft Streaming Clock  
Proxy,system32\drivers\MSPCLOCK.sys,Kernel driver,Manual,  
Sun Feb 14 15:57:33 2016Z,MSTEE,Microsoft Streaming Tee/Sink-to-Sink  
Converter,system32\drivers\MSTEE.sys,Kernel driver,Manual,  
Wed Feb 10 01:34:39 2016Z,tap0901,TAP-Windows Adapter  
V9,system32\DRIVERS\tap0901.sys,Kernel driver,Manual,  
Tue Feb 9 22:07:39 2016Z,clr\_optimization\_v2.0.50727\_32,Microsoft .NET Framework  
NGEN  
v2.0.50727\_X86,%systemroot%\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe,Own\_Proc  
ess,Disabled,LocalSystem  
Tue Feb 9 22:07:39 2016Z,clr\_optimization\_v2.0.50727\_64,Microsoft .NET Framework  
NGEN  
v2.0.50727\_X64,%systemroot%\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe,Own\_Pr  
ocess,Disabled,LocalSystem  
Wed Feb 3 04:32:57  
2016Z,BITS,@%SystemRoot%\system32\qmgr.dll;-1000,%SystemRoot%\System32\svchost.exe  
-k netsvcs,Share\_Process,Auto Start,LocalSystem  
Tue Feb 2 00:31:05 2016Z,BrYNSvc,BrYNSvc,"C:\Program Files  
(x86)\Brown02\BrYNSvc.exe",Own\_Process,Manual,LocalSystem  
Tue Feb 2 00:20:01 2016Z,PDFProFiltSrvPP,PDFProFiltSrvPP,C:\Program Files  
(x86)\Nuance\PaperPort\PDFProFiltSrvPP.exe,Own\_Process,Auto Start,LocalSystem  
Mon Feb 1 03:04:18 2016Z,StillCam,Still Serial Digital Camera  
Driver,system32\DRIVERS\serscan.sys,Kernel driver,Manual,  
Tue Jan 19 22:34:35 2016Z,IntuitUpdateServiceV4,Intuit Update Service v4,"C:\Program  
Files (x86)\Common Files\Intuit\Update Service  
v4\IntuitUpdateService.exe",Own\_Process,Auto Start,LocalSystem  
Tue Jan 19 22:14:22  
2016Z,msiserver,@%SystemRoot%\system32\msimg.dll;-27,%systemroot%\system32\msiexec.  
exe /V,Own\_Process,Auto Start,LocalSystem  
Thu Jan 7 22:15:30 2016Z,iPod Service,iPod Service,"C:\Program  
Files\iPod\bin\iPodService.exe",Own\_Process,Manual,LocalSystem  
Thu Jan 7 22:11:07 2016Z,Bonjour Service,Bonjour Service,"C:\Program  
Files\Bonjour\mDNSResponder.exe",Own\_Process,Auto Start,LocalSystem  
Fri Jan 1 20:52:19 2016Z,MozillaMaintenance,Mozilla Maintenance Service,"C:\Program  
Files (x86)\Mozilla Maintenance  
Service\maintenanceservice.exe",Own\_Process,Manual,LocalSystem  
Sat Nov 28 20:21:16 2015Z,{1BDD94C3-9D85-46F0-87E3-BD3288A5F6BD},,,,,,  
Wed Nov 11 20:32:01  
2015Z,SharedAccess\Parameters,,%SystemRoot%\System32\ipnathlp.dll,,,  
Wed Nov 11 20:31:53  
2015Z,SharedAccess,@%SystemRoot%\system32\ipnathlp.dll;-106,%SystemRoot%\System32\sv  
chost.exe -k netsvcs,Share\_Process,Manual,LocalSystem  
Wed Nov 11 20:31:50 2015Z,{A9E50A43-973B-4CAD-B78E-EA0321A4A293},,,,,,  
Mon Oct 19 23:21:21 2015Z,MSDTC Bridge 4.0.0.0,,,,,  
Mon Oct 19 23:21:21 2015Z,SMScvHost 4.0.0.0,,,,,  
Mon Oct 19 23:21:21 2015Z,Windows Workflow Foundation 4.0.0.0,,,,,  
Fri Oct 2 14:28:51 2015Z,McODS,McAfee Scanner,"C:\Program  
Files\McAfee\VirusScan\mcods.exe",Own\_Process,Manual,LocalSystem

## SYSTEM OUTPUT

Wed Sep 23 03:20:38 2015Z,usbvideo,USB Video Device  
 (WDM),System32\Drivers\usbvideo.sys,Kernel driver,Manual,  
 Sat Sep 12 00:14:59 2015Z,ASP.NET,,,,,  
 Sat Sep 12 00:14:57 2015Z,ASP.NET\_4.0.30319,,,,,  
 Sat Sep 12 00:14:57 2015Z,aspnet\_state,ASP.NET State  
 Service,%SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\aspnet\_state.exe,Own\_Proce  
 ss,Disabled,NT AUTHORITY\NetworkService  
 Sat Sep 12 00:14:30  
 2015Z,NetMsmqActivator,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceMode  
 lInstallRC.dll;-8195,"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMsvchost.exe"  
 -NetMsmqActivator,Share\_Process,Disabled,NT AUTHORITY\NetworkService  
 Sat Sep 12 00:14:29  
 2015Z,NetPipeActivator,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceMode  
 lInstallRC.dll;-8197,C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMsvchost.exe,S  
 hare\_Process,Disabled,NT AUTHORITY\LocalService  
 Sat Sep 12 00:14:25  
 2015Z,NetTcpActivator,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceModel  
 InstallRC.dll;-8199,C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMsvchost.exe,Sh  
 are\_Process,Disabled,NT AUTHORITY\LocalService  
 Sat Sep 12 00:14:23  
 2015Z,NetTcpPortSharing,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\\ServiceMod  
 elInstallRC.dll;-8201,C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMsvchost.exe,  
 Share\_Process,Disabled,NT AUTHORITY\LocalService  
 Sat Sep 12 00:14:19 2015Z,.NET Memory Cache 4.0,,,,,  
 Sat Sep 12 00:09:28  
 2015Z,stisvc,@%SystemRoot%\system32\wiaservc.dll;-9,%SystemRoot%\system32\svchost.exe  
 -k imgsvc,Own\_Process,Auto Start,NT Authority\LocalService  
 Fri Sep 11 18:30:16 2015Z,Apple Mobile Device,,,,,  
 Fri Sep 11 17:57:59 2015Z,Apple Mobile Device Service,Apple Mobile Device  
 Service,"C:\Program Files\Common Files\Apple\Mobile Device  
 Support\AppleMobileDeviceService.exe",Own\_Process,Auto Start,LocalSystem  
 Fri Sep 11 14:56:27 2015Z,gupdate,Google Update Service (gupdate),"C:\Program Files  
 (x86)\Google\Update\GoogleUpdate.exe" /svc,Own\_Process,Auto Start,LocalSystem  
 Fri Sep 11 14:56:27 2015Z,gupdatem,Google Update Service (gupdatem),"C:\Program  
 Files (x86)\Google\Update\GoogleUpdate.exe" /medsvc,Own\_Process,Manual,LocalSystem  
 Fri Sep 11 07:47:27  
 2015Z,WbioSrv,>@%systemroot%\system32\wbiosrv.dll;-100,%SystemRoot%\system32\svchos  
 t.exe -k WbioSvcGroup,Share\_Process,Manual,LocalSystem  
 Thu Sep 10 21:49:02 2015Z,clr\_optimization\_v4.0.30319\_64,Microsoft .NET Framework  
 NGEN  
 v4.0.30319\_X64,C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe,Own\_Proc  
 ess,Auto Start,LocalSystem  
 Thu Sep 10 21:49:01 2015Z,clr\_optimization\_v4.0.30319\_32,Microsoft .NET Framework  
 NGEN  
 v4.0.30319\_X86,C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe,Own\_Proces  
 s,Auto Start,LocalSystem  
 Thu Sep 10 21:48:06 2015Z,.NET CLR Networking 4.0.0.0,,,,,  
 Thu Sep 10 21:30:14



## SYSTEM OUTPUT

2015Z,eventlog,@%SystemRoot%\system32\wevtsvc.dll;-200,%SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted,Share\_Process,Auto Start,NT  
 AUTHORITY\LocalService  
 Thu Sep 10 21:30:14 2015Z,Outlook,,,,,  
 Thu Sep 10 21:28:37 2015Z,osppsvc,Office Software Protection Platform,"C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE",Own\_Process,Manual,NT  
 AUTHORITY\NetworkService  
 Thu Sep 10 20:46:43  
 2015Z,DiagTrack,@%SystemRoot%\system32\UtcResources.dll;-3001,%SystemRoot%\System32\svchost.exe -k utcsvc,Own\_Process,Auto Start,LocalSystem  
 Thu Sep 10 20:46:43  
 2015Z,DiagTrack\Parameters,,%SystemRoot%\system32\diagtrack.dll,,,  
 Thu Sep 10 19:42:05 2015Z,ose,Office Source Engine,"C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE",Own\_Process,Manual,LocalSystem  
 Thu Sep 10 17:10:15  
 2015Z,IKEEXT,@%SystemRoot%\system32\ikeext.dll;-501,%systemroot%\system32\svchost.exe -k netsvcs,Share\_Process,Auto Start,LocalSystem  
 Thu Sep 10 17:09:34 2015Z,HipShieldK,McAfee Inc.  
 HipShieldK,system32\drivers\HipShieldK.sys,Kernel driver,Manual,  
 Thu Sep 10 16:33:32 2015Z,odserv,Microsoft Office Diagnostics Service,"C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\ODSERV.EXE",Own\_Process,Manual,LocalSystem  
 Thu Sep 10 04:09:03 2015Z,WMPNetworkSvc,@%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe;-101,"%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe",Own\_Process,Auto Start,NT AUTHORITY\NetworkService  
 Thu Sep 10 04:09:02  
 2015Z,HomeGroupListener,@%SystemRoot%\System32\ListSvc.dll;-100,%SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted,Share\_Process,Manual,LocalSystem  
 Thu Sep 10 04:08:46  
 2015Z,FDResPub,@%systemroot%\system32\fdrespub.dll;-100,%SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation,Share\_Process,Auto Start,NT  
 AUTHORITY\LocalService  
 Thu Sep 3 18:12:30  
 2015Z,WSearch,@%systemroot%\system32\SearchIndexer.exe;-103,%systemroot%\system32\SearchIndexer.exe /Embedding,Own\_Process,Auto Start,LocalSystem  
 Thu Sep 3 17:49:58  
 2015Z,CertPropSvc,@%SystemRoot%\System32\certprop.dll;-11,%SystemRoot%\system32\svchost.exe -k netsvcs,Share\_Process,Auto Start,LocalSystem  
 Thu Sep 3 17:49:58  
 2015Z,SCardSvr,@%SystemRoot%\System32\SCardSvr.dll;-1,%SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation,Share\_Process,Auto Start,NT  
 AUTHORITY\LocalService  
 Thu Sep 3 17:49:37 2015Z,{720B974A-3E6B-42BF-9839-4EE6CD676477},,,,,,  
 Fri Feb 20 18:42:20 2015Z,adp94xx,,\SystemRoot\system32\drivers\adp94xx.sys,Kernel driver,Manual,  
 Fri Feb 20 18:42:20 2015Z,adpahci,,\SystemRoot\system32\drivers\adpahci.sys,Kernel driver,Manual,

## SYSTEM OUTPUT

Fri Feb 20 18:42:20 2015Z,adpu320,,\SystemRoot\system32\drivers\adpu320.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,aliide,,\SystemRoot\system32\drivers\aliide.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,amdide,,\SystemRoot\system32\drivers\amdide.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,amdsata,,\SystemRoot\system32\drivers\amdsata.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,amdsbs,,\SystemRoot\system32\drivers\amdsbs.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,arc,,\SystemRoot\system32\drivers\arc.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,arcsas,,\SystemRoot\system32\drivers\arcsas.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,cmdide,,\SystemRoot\system32\drivers\cmdide.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,elxstor,,\SystemRoot\system32\drivers\elxstor.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,HpSAMD,,\SystemRoot\system32\drivers\HpSAMD.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,iaStorV,,\SystemRoot\system32\drivers\iaStorV.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,iirsp,,\SystemRoot\system32\drivers\iirsp.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,intelide,,\SystemRoot\system32\drivers\intelide.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,isapnp,,\SystemRoot\system32\drivers\isapnp.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,LSI\_FC,,\SystemRoot\system32\drivers\lsi\_fc.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,LSI\_SAS,,\SystemRoot\system32\drivers\lsi\_sas.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,LSI\_SAS2,,\SystemRoot\system32\drivers\lsi\_sas2.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,LSI\_SCSI,,\SystemRoot\system32\drivers\lsi\_scsi.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,megasas,,\SystemRoot\system32\drivers\megasas.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,MegaSR,,\SystemRoot\system32\drivers\MegaSR.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,mpio,,\SystemRoot\system32\drivers\mpio.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,msdsm,,\SystemRoot\system32\drivers\msdsm.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,nfrd960,,\SystemRoot\system32\drivers\nfrd960.sys,Kernel driver,Manual,  
Fri Feb 20 18:42:20 2015Z,nvraid,,\SystemRoot\system32\drivers\nvraid.sys,Kernel driver,Manual,

## SYSTEM OUTPUT

```

Fri Feb 20 18:42:20 2015Z,nvstor,,\SystemRoot\system32\drivers\nvstor.sys,Kernel
driver,Manual,
Fri Feb 20 18:42:20 2015Z,pciide,,\SystemRoot\system32\drivers\pciide.sys,Kernel
driver,Manual,
Fri Feb 20 18:42:20 2015Z,ql2300,,\SystemRoot\system32\drivers\ql2300.sys,Kernel
driver,Manual,
Fri Feb 20 18:42:20 2015Z,ql40xx,,\SystemRoot\system32\drivers\ql40xx.sys,Kernel
driver,Manual,
Fri Feb 20 18:42:20 2015Z,sbp2port,,\SystemRoot\system32\drivers\sbp2port.sys,Kernel
driver,Manual,
Fri Feb 20 18:42:20 2015Z,SiSRaid2,,\SystemRoot\system32\drivers\SiSRaid2.sys,Kernel
driver,Manual,
Fri Feb 20 18:42:20 2015Z,SiSRaid4,,\SystemRoot\system32\drivers\sisraid4.sys,Kernel
driver,Manual,
Fri Feb 20 18:42:20 2015Z,stexstor,,\SystemRoot\system32\drivers\stexstor.sys,Kernel
driver,Manual,
Fri Feb 20 18:42:20 2015Z,storvsc,,\SystemRoot\system32\drivers\storvsc.sys,Kernel
driver,Manual,
Fri Feb 20 18:42:20 2015Z,viaide,,\SystemRoot\system32\drivers\viaide.sys,Kernel
driver,Manual,
Fri Feb 20 18:42:20 2015Z,vmbus,,\SystemRoot\system32\drivers\vmbus.sys,Kernel
driver,Manual,
Fri Feb 20 18:42:20 2015Z,vsmraid,,\SystemRoot\system32\drivers\vsmraid.sys,Kernel
driver,Manual,
Fri Feb 20 18:42:20 2015Z,Wd,,\SystemRoot\system32\drivers\wd.sys,Kernel
driver,Manual,
Fri Feb 20 18:42:17
2015Z,EapHost,@%systemroot%\system32\eapsvc.dll;-1,%SystemRoot%\System32\svchost.exe
-k netsvcs,Share_Process,Manual,localSystem
Fri Feb 20 18:42:17 2015Z,terminpt,Microsoft Remote Desktop Input
Driver,\SystemRoot\system32\drivers\terminpt.sys,Kernel driver,Manual,
Fri Feb 20 18:42:17 2015Z,TsUsbGD,Remote Desktop Generic USB
Device,\SystemRoot\system32\drivers\TsUsbGD.sys,Kernel driver,Manual,
Fri Feb 20 18:23:16 2015Z,cphs,Intel(R) Content Protection HECI
Service,%SystemRoot%\SysWow64\IntelCpHeciSvc.exe,Own_Process,Manual,LocalSystem
Fri Feb 20 18:22:35 2015Z,{FD2B5103-617C-4AE6-8DC4-A4772C463DDC},,,,,
Fri Feb 20 17:05:34 2015Z,vcsFPSvc,Validity VCS Fingerprint
Service,C:\Windows\system32\vcsFPSvc.exe,Own_Process,Auto Start,LocalSystem
Fri Feb 20 16:54:33 2015Z,AtiHDAudioService,AMD Function Driver for HD Audio
Service,system32\drivers\AtihdW76.sys,Kernel driver,Manual,
Fri Feb 20 16:54:27 2015Z,amdkmddap,,system32\DRIVERS\atikmpag.sys,Kernel
driver,Manual,
Fri Feb 20 16:54:14 2015Z,{3ED9F155-8201-430C-85E1-EDD7020DE0CF},,,,,
Fri Feb 20 16:53:55 2015Z,AMD External Events
Utility,,%SystemRoot%\system32\atiesrxx.exe,Own_Process,Auto Start,LocalSystem
Fri Feb 20 16:53:55 2015Z,Atierecord,,,,,
Fri Feb 20 16:53:55 2015Z,iphlpvc\Parameters,,%SystemRoot%\System32\iphlpvc.dll,,,
Fri Feb 20 16:53:49 2015Z,{8B32CCEF-F092-453D-A04B-084246668014},,,,,

```

## SYSTEM OUTPUT

Fri Feb 20 16:53:43 2015Z,{749B2830-EBF4-4268-8BFD-189D3224ACFB},,,,,  
 Fri Feb 20 16:53:35 2015Z,hpsrv,HP  
 Service,%SystemRoot%\system32\Hpservice.exe,Own\_Process,Auto Start,LocalSystem  
 Fri Feb 20 16:53:06 2015Z,ohci1394,1394 OHCI Compliant Host Controller  
 (Legacy),\SystemRoot\system32\drivers\ohci1394.sys,Kernel driver,Manual,  
 Mon Dec 1 14:38:46  
 2014Z,SysMain,@%SystemRoot%\system32\sysmain.dll;-1000,%systemroot%\system32\svchost  
 .exe -k LocalSystemNetworkRestricted,Share\_Process,Auto Start,LocalSystem  
 Mon Dec 1 14:16:45  
 2014Z,WatAdminSvc,@%SystemRoot%\system32\Wat\WatUX.exe;-601,%SystemRoot%\system32\Wa  
 t\WatAdminSvc.exe,Own\_Process,Manual,LocalSystem  
 Mon Dec 1 14:14:27 2014Z,gpsvc,@gpapi.dll;-112,%windir%\system32\svchost.exe -k  
 GPSvcGroup,Own\_Process,Auto Start,LocalSystem  
 Mon Dec 1 14:13:22  
 2014Z,IEEtwCollectorService,@%SystemRoot%\system32\ieetwcollectorres.dll;-1000,%Syst  
 emRoot%\system32\IEEtwCollector.exe /V,Own\_Process,Manual,LocalSystem  
 Mon Dec 1 14:13:22 2014Z,RDPUDD,,,,,  
 Mon Dec 1 14:13:22 2014Z,RdpVideoMiniport,Remote Desktop Video Miniport  
 Driver,System32\drivers\rdpvideominiport.sys,Kernel driver,Manual,  
 Mon Dec 1 14:13:22 2014Z,WinHttpAutoProxySvc\Parameters,,winhttp.dll,,  
 Mon Dec 1 14:01:16 2014Z,MSDTC Bridge 3.0.0.0,,,,,  
 Mon Dec 1 14:01:16 2014Z,ServiceModelEndpoint 3.0.0.0,,,,,  
 Mon Dec 1 14:01:16 2014Z,ServiceModelOperation 3.0.0.0,,,,,  
 Mon Dec 1 14:01:16 2014Z,ServiceModelService 3.0.0.0,,,,,  
 Mon Dec 1 14:01:16 2014Z,SMSSvcHost 3.0.0.0,,,,,  
 Mon Dec 1 14:01:16 2014Z,Windows Workflow Foundation 3.0.0.0,,,,,  
 Mon Dec 1 13:04:59  
 2014Z,wuauserv,@%systemroot%\system32\wuaueng.dll;-105,%systemroot%\system32\svchost  
 .exe -k netsvcs,Share\_Process,Auto Start,LocalSystem  
 Mon Dec 1 13:00:30 2014Z,Wlansvc\Parameters,,%SystemRoot%\System32\wlansvc.dll,,  
 Mon Dec 1 12:59:32 2014Z,BTHPORT,Bluetooth Port  
 Driver,System32\Drivers\BTHport.sys,Kernel driver,Manual,  
 Mon Dec 1 12:59:19  
 2014Z,Wlansvc,@%SystemRoot%\System32\wlansvc.dll;-257,%SystemRoot%\system32\svchost.  
 exe -k LocalSystemNetworkRestricted,Share\_Process,Auto Start,LocalSystem  
 Sat Nov 29 16:11:45  
 2014Z,WebClient,@%systemroot%\system32\webclnt.dll;-100,%SystemRoot%\system32\svchos  
 t.exe -k LocalService,Share\_Process,Manual,NT AUTHORITY\LocalService  
 Sat Nov 29 16:10:13 2014Z,ProfSvc\Parameters,,%systemroot%\system32\profsvc.dll,,  
 Sat Nov 29 16:10:13 2014Z,WebClient\Parameters,,%SystemRoot%\System32\webclnt.dll,,  
 Sat Nov 29 16:07:24  
 2014Z,wudfsvc,@%SystemRoot%\system32\wudfsvc.dll;-1000,%SystemRoot%\system32\svchost  
 .exe -k LocalSystemNetworkRestricted,Share\_Process,Manual,LocalSystem  
 Sat Nov 29 16:06:59  
 2014Z,FontCache,@%systemroot%\system32\FntCache.dll;-100,%SystemRoot%\system32\svcho  
 st.exe -k LocalService,Share\_Process,Auto Start,NT AUTHORITY\LocalService  
 Sat Nov 29 16:06:59  
 2014Z,FontCache\Parameters,,%SystemRoot%\system32\FntCache.dll,,

## SYSTEM OUTPUT

Tue Apr 12 08:29:05  
 2011Z,CscService,@%systemroot%\system32\csccsvc.dll;-200,%SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted,Share\_Process,Auto Start,LocalSystem

Tue Apr 12 08:28:48  
 2011Z,AppMgmt,@appmgmts.dll;-3250,%SystemRoot%\system32\svchost.exe -k netsvcs,Share\_Process,Manual,LocalSystem

Tue Apr 12 08:28:48  
 2011Z,ehRecvr,@%SystemRoot%\ehome\ehrecvr.exe;-101,%systemroot%\ehome\ehRecvr.exe,Own\_Process,Manual,NT AUTHORITY\networkService

Tue Apr 12 08:28:48  
 2011Z,ehSched,@%SystemRoot%\ehome\ehsched.exe;-101,%systemroot%\ehome\ehsched.exe,Own\_Process,Manual,NT AUTHORITY\networkService

Tue Apr 12 08:28:48  
 2011Z,Mcx2Svc,@%SystemRoot%\ehome\ehres.dll;-15501,%SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation,Share\_Process,Disabled,NT Authority\LocalService

Tue Apr 12 08:28:48  
 2011Z,PeerDistSvc,@%SystemRoot%\system32\peerdistsvc.dll;-9000,%SystemRoot%\System32\svchost.exe -k PeerDist,Share\_Process,Manual,NT AUTHORITY\NetworkService

Tue Apr 12 08:28:48 2011Z,RDPDR,Terminal Server Device Redirector Driver,System32\drivers\rdpdr.sys,Kernel driver,Manual,

Tue Apr 12 08:28:48  
 2011Z,SensrSvc,@%SystemRoot%\System32\sensrsvc.dll;-1000,%SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation,Share\_Process,Manual,NT AUTHORITY\LocalService

Tue Apr 12 08:28:48  
 2011Z,StorSvc,@%SystemRoot%\System32\StorSvc.dll;-100,%SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted,Share\_Process,Manual,LocalSystem

Tue Apr 12 08:28:48  
 2011Z,UmRdpService,@%SystemRoot%\system32\umrdp.dll;-1000,%SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted,Share\_Process,Manual,localSystem

Tue Apr 12 08:28:45 2011Z,AppMgmt\Parameters,,%SystemRoot%\System32\appmgmts.dll,,,  
 Tue Apr 12 08:28:45 2011Z,CscService\Parameters,,%SystemRoot%\System32\csccsvc.dll,,,  
 Tue Apr 12 08:28:45 2011Z,Mcx2Svc\Parameters,,%SystemRoot%\system32\Mcx2Svc.dll,,,  
 Tue Apr 12 08:28:45 2011Z,PeerDistSvc\Parameters,,%SystemRoot%\system32\peerdistsvc.dll,,,  
 Tue Apr 12 08:28:45 2011Z,SensrSvc\Parameters,,%SystemRoot%\system32\sensrsvc.dll,,,  
 Tue Apr 12 08:28:45 2011Z,StorSvc\Parameters,,%SystemRoot%\system32\storsvc.dll,,,  
 Tue Apr 12 08:28:45 2011Z,UmRdpService\Parameters,,%SystemRoot%\System32\umrdp.dll,,,  
 Tue Apr 12 08:27:52 2011Z,dmvs, \SystemRoot\system32\drivers\dmvs.sys,Kernel driver,Manual,  
 Tue Apr 12 08:27:52 2011Z,s3cap,, \SystemRoot\system32\drivers\vms3cap.sys,Kernel driver,Manual,  
 Tue Apr 12 08:27:52 2011Z,VBuSHID,, \SystemRoot\system32\drivers\VBuSHID.sys,Kernel driver,Manual,  
 Sun Nov 21 03:58:24 2010Z,BTHMODEM,Bluetooth Serial Communications Driver,\SystemRoot\system32\drivers\bthmodem.sys,Kernel driver,Manual,  
 Sun Nov 21 03:58:22 2010Z,gagp30kx,Microsoft Generic AGPv3.0 Filter for K8 Processor

## SYSTEM OUTPUT

Platforms, \SystemRoot\system32\drivers\gagp30kx.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:22 2010Z, uagp35, Microsoft AGPv3.5  
 Filter, \SystemRoot\system32\drivers\uagp35.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:21 2010Z, b06bdrv, Broadcom NetXtreme II  
 VBD, \SystemRoot\system32\drivers\bxbvda.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:21 2010Z, HidBth, Microsoft Bluetooth HID  
 Miniport, \SystemRoot\system32\drivers\hidbth.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:19 2010Z, AmdK8, AMD K8 Processor  
 Driver, \SystemRoot\system32\drivers\amdk8.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:19 2010Z, AmdPPM, AMD Processor  
 Driver, \SystemRoot\system32\drivers\amdppm.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:19 2010Z, Processor, Processor  
 Driver, \SystemRoot\system32\drivers\processr.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:18 2010Z, ebdrv, Broadcom NetXtreme II 10 Gige  
 VBD, \SystemRoot\system32\drivers\evbda.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:18 2010Z, fdc, Floppy Disk Controller  
 Driver, \SystemRoot\system32\drivers\fdc.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:17 2010Z, pcmcia, , \SystemRoot\system32\drivers\pcmcia.sys, Kernel  
 driver, Manual,  
 Sun Nov 21 03:58:16 2010Z, MTConfig, Microsoft Input Configuration  
 Driver, \SystemRoot\system32\drivers\MTConfig.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:15 2010Z, circlass, Consumer IR  
 Devices, \SystemRoot\system32\drivers\circlass.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:13 2010Z, flpydisk, Floppy Disk  
 Driver, \SystemRoot\system32\drivers\flpydisk.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:13 2010Z, sfloppy, High-Capacity Floppy Disk  
 Drive, \SystemRoot\system32\drivers\sfloppy.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:11 2010Z, HidBatt, HID UPS Battery  
 Driver, \SystemRoot\system32\drivers\HidBatt.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:08 2010Z, HidIr, Microsoft Infrared HID  
 Driver, \SystemRoot\system32\drivers\hidir.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:07 2010Z, sermouse, Serial Mouse  
 Driver, \SystemRoot\system32\drivers\sermouse.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:06 2010Z, BrFiltLo, Brother USB Mass-Storage Lower Filter  
 Driver, \SystemRoot\system32\drivers\BrFiltLo.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:06 2010Z, BrFiltUp, Brother USB Mass-Storage Upper Filter  
 Driver, \SystemRoot\system32\drivers\BrFiltUp.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:05 2010Z, usbohci, Microsoft USB Open Host Controller Miniport  
 Driver, \SystemRoot\system32\drivers\usbohci.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:05 2010Z, usbuhci, Microsoft USB Universal Host Controller Miniport  
 Driver, \SystemRoot\system32\drivers\usbuhci.sys, Kernel driver, Manual,  
 Sun Nov 21 03:58:00 2010Z, WacomPen, Wacom Serial Pen HID  
 Driver, \SystemRoot\system32\drivers\wacompen.sys, Kernel driver, Manual,  
 Sun Nov 21 03:57:59 2010Z, crcdisk, Crcdisk Filter  
 Driver, \SystemRoot\system32\drivers\crcdisk.sys, Kernel driver, Disabled,  
 Sun Nov 21 03:57:58 2010Z, UmPass, Microsoft UMPass  
 Driver, \SystemRoot\system32\drivers\umpass.sys, Kernel driver, Manual,  
 Sun Nov 21 03:46:56 2010Z, b57nd60a, Broadcom NetXtreme Gigabit Ethernet - NDIS

## SYSTEM OUTPUT

6.0,system32\DRIVERS\b57nd60a.sys,Kernel driver,Manual,  
 Sun Nov 21 03:46:56 2010Z,vga,,system32\DRIVERS\vganp.sys,Kernel driver,Manual,  
 Sun Nov 21 03:39:53 2010Z,Dhcp\Parameters,,%SystemRoot%\system32\dhcpcore.dll,,,  
 Sun Nov 21 03:38:46 2010Z,TsUsbFlt,,system32\drivers\tsusbflt.sys,Kernel  
 driver,Manual,  
 Sun Nov 21 03:33:56  
 2010Z,SessionEnv,@%SystemRoot%\System32\SessEnv.dll;-1026,%SystemRoot%\System32\svch  
 ost.exe -k netsvcs,Share\_Process,Manual,localSystem  
 Sun Nov 21 03:29:32 2010Z,AcpiPmi,ACPI Power Meter  
 Driver,\SystemRoot\system32\drivers\acpipmi.sys,Kernel driver,Manual,  
 Sun Nov 21 03:29:32 2010Z,agp440,Intel AGP Bus  
 Filter,\SystemRoot\system32\drivers\agp440.sys,Kernel driver,Manual,  
 Sun Nov 21 03:29:32 2010Z,amdxata,,system32\drivers\amdxata.sys,Kernel driver,Boot  
 Start,  
 Sun Nov 21 03:29:32 2010Z,ErrDev,Microsoft Hardware Error Device  
 Driver,\SystemRoot\system32\drivers\errdev.sys,Kernel driver,Manual,  
 Sun Nov 21 03:29:32 2010Z,IPMIDRV,,\SystemRoot\system32\drivers\IPMIDrv.sys,Kernel  
 driver,Manual,  
 Sun Nov 21 03:29:32 2010Z,iScsiPrt,iScsiPort  
 Driver,\SystemRoot\system32\drivers\msiscsi.sys,Kernel driver,Manual,  
 Sun Nov 21 03:29:32 2010Z,nv\_agp,NVIDIA nForce AGP Bus  
 Filter,\SystemRoot\system32\drivers\nv\_agp.sys,Kernel driver,Manual,  
 Sun Nov 21 03:29:32 2010Z,sffdisk,SFF Storage Class  
 Driver,\SystemRoot\system32\drivers\sffdisk.sys,Kernel driver,Manual,  
 Sun Nov 21 03:29:32 2010Z,sffp\_mmc,SFF Storage Protocol Driver for  
 MMC,\SystemRoot\system32\drivers\sffp\_mmc.sys,Kernel driver,Manual,  
 Sun Nov 21 03:29:32 2010Z,sffp\_sd,SFF Storage Protocol Driver for  
 SDBus,\SystemRoot\system32\drivers\sffp\_sd.sys,Kernel driver,Manual,  
 Sun Nov 21 03:29:32 2010Z,uliagpkx,Uli AGP Bus  
 Filter,\SystemRoot\system32\drivers\uliagpkx.sys,Kernel driver,Manual,  
 Sun Nov 21 03:29:32 2010Z,usbcir,eHome Infrared Receiver  
 (USBCIR),\SystemRoot\system32\drivers\usbcir.sys,Kernel driver,Manual,  
 Sun Nov 21 03:29:32 2010Z,vhdmpp,,\SystemRoot\system32\drivers\vhdmpp.sys,Kernel  
 driver,Manual,  
 Tue Jul 14 05:34:12 2009Z,BDESVC\Parameters,,%SystemRoot%\System32\bdesvc.dll,,,  
 Tue Jul 14 05:34:12  
 2009Z,PNRPAutoReg\Parameters,,%SystemRoot%\system32\pnrpauto.dll,,,  
 Tue Jul 14 05:34:12 2009Z,WPCSvc\Parameters,,%SystemRoot%\System32\wpcsvc.dll,,,  
 Tue Jul 14 05:34:09 2009Z,p2pimsvc\Parameters,,%SystemRoot%\system32\pnrpmsvc.dll,,,  
 Tue Jul 14 05:34:09 2009Z,p2psvc\Parameters,,%SystemRoot%\system32\p2psvc.dll,,,  
 Tue Jul 14 05:34:09 2009Z,SDRSVC\Parameters,,%Systemroot%\System32\SDRSVC.dll,,,  
 Tue Jul 14 04:54:38 2009Z,NdisCap,NDIS Capture LightWeight  
 Filter,system32\DRIVERS\ndiscap.sys,Kernel driver,Manual,  
 Tue Jul 14 04:54:32 2009Z,hkmsvc\Parameters,,%SystemRoot%\system32\kmsvc.dll,,,  
 Tue Jul 14 04:54:31 2009Z,napagent\Parameters,,%SystemRoot%\system32\qagentRT.dll,,,  
 Tue Jul 14 04:54:25  
 2009Z,defragSvc\Parameters,,%Systemroot%\System32\defragSvc.dll,,,  
 Tue Jul 14 04:54:05 2009Z,WerSvc\Parameters,,%SystemRoot%\System32\WerSvc.dll,,,

## SYSTEM OUTPUT

```

Tue Jul 14 04:53:57
2009Z,Smb,@%SystemRoot%\system32\tcpipcfg.dll;-50005,system32\DRIVERS\smb.sys,Kernel
driver,Manual,
Tue Jul 14 04:53:56 2009Z,lmhosts\Parameters,,%SystemRoot%\System32\lmhsvc.dll,,,
Tue Jul 14 04:53:48 2009Z,THREADORDER\Parameters,,%SystemRoot%\system32\mmcscs.dll,,,
Tue Jul 14 04:53:45
2009Z,TrkWks,@%SystemRoot%\system32\trkwks.dll;-1,%SystemRoot%\System32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:53:45 2009Z,TrkWks\Parameters,,%SystemRoot%\System32\trkwks.dll,,,
Tue Jul 14 04:53:36
2009Z,RpcEptMapper,@%windir%\system32\RpcEpMap.dll;-1001,%SystemRoot%\system32\svcho
st.exe -k RPCSS,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Tue Jul 14 04:53:36
2009Z,RpcEptMapper\Parameters,,%SystemRoot%\System32\RpcEpMap.dll,,,
Tue Jul 14 04:53:33
2009Z,LanmanServer,@%systemroot%\system32\srvsvc.dll;-100,%SystemRoot%\system32\svch
ost.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:53:31
2009Z,LanmanWorkstation,@%systemroot%\system32\wkssvc.dll;-100,%SystemRoot%\System32
\svchost.exe -k NetworkService,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Tue Jul 14 04:53:31
2009Z,LanmanWorkstation\Parameters,,%SystemRoot%\System32\wkssvc.dll,,,
Tue Jul 14 04:53:25 2009Z,WmiApRpl,,,,,
Tue Jul 14 04:53:24
2009Z,Winmgmt,@%Systemroot%\system32\wbem\wmisvc.dll;-205,%systemroot%\system32\svch
ost.exe -k netsvcs,Share_Process,Auto Start,localSystem
Tue Jul 14 04:53:24
2009Z,wmiApSrv,@%Systemroot%\system32\wbem\wmiapsrv.exe;-110,%systemroot%\system32\w
bem\WmiApSrv.exe,Own_Process,Manual,localSystem
Tue Jul 14 04:53:21 2009Z,TCPIP6,Microsoft IPv6 Protocol
Driver,system32\DRIVERS\tcpip.sys,Kernel driver,Manual,
Tue Jul 14 04:53:21
2009Z,WANARP,@%systemroot%\system32\rascfg.dll;-32011,system32\DRIVERS\wanarp.sys,Ke
rnel driver,Manual,
Tue Jul 14 04:53:20
2009Z,lmhosts,@%SystemRoot%\system32\lmhsvc.dll;-101,%SystemRoot%\system32\svchost.e
xe -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService
Tue Jul 14 04:53:19
2009Z,Dhcp,@%SystemRoot%\system32\dhcpcore.dll;-100,%SystemRoot%\system32\svchost.ex
e -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
Authority\LocalService
Tue Jul 14 04:53:19 2009Z,Winsock,,,Adapter,Manual,
Tue Jul 14 04:49:48
2009Z,SamSs,@%SystemRoot%\system32\samsrv.dll;-1,%SystemRoot%\system32\lsass.exe,Sha
re_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:48
2009Z,W32Time,@%SystemRoot%\system32\w32time.dll;-200,%SystemRoot%\system32\svchost.

```



## SYSTEM OUTPUT

```

exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:48 2009Z,W32Time\Parameters,,%systemroot%\system32\w32time.dll,,,
Tue Jul 14 04:49:46
2009Z,Dnscache,@%SystemRoot%\System32\dnsapi.dll;-101,%SystemRoot%\system32\svchost.
exe -k NetworkService,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:46 2009Z,Dnscache\Parameters,,%SystemRoot%\System32\dnssrslvr.dll,,,
Tue Jul 14 04:49:45
2009Z,RemoteAccess,@%Systemroot%\system32\mprdim.dll;-200,%SystemRoot%\System32\svch
ost.exe -k netsvcs,Share_Process,Disabled,localSystem
Tue Jul 14 04:49:45
2009Z,RemoteAccess\Parameters,,%SystemRoot%\System32\mprdim.dll,,,
Tue Jul 14 04:49:35
2009Z,RasAuto,@%Systemroot%\system32\rasauto.dll;-200,%SystemRoot%\System32\svchost.
exe -k netsvcs,Share_Process,Manual,localSystem
Tue Jul 14 04:49:35 2009Z,RasAuto\Parameters,,%SystemRoot%\System32\rasauto.dll,,,
Tue Jul 14 04:49:35
2009Z,RasMan,@%Systemroot%\system32\rasmans.dll;-200,%SystemRoot%\System32\svchost.e
xe -k netsvcs,Share_Process,Manual,localSystem
Tue Jul 14 04:49:35 2009Z,RasMan\Parameters,,%SystemRoot%\System32\rasmans.dll,,,
Tue Jul 14 04:49:26 2009Z,SstpSvc\Parameters,,%SystemRoot%\system32\sstpsvc.dll,,,
Tue Jul 14 04:49:24
2009Z,DPS,@%systemroot%\system32\dps.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Auto Start,NT AUTHORITY\LocalService
Tue Jul 14 04:49:24 2009Z,DPS\Parameters,,%SystemRoot%\system32\dps.dll,,,
Tue Jul 14 04:49:24
2009Z,WdiServiceHost,@%systemroot%\system32\wdi.dll;-502,%SystemRoot%\System32\svcho
st.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:24
2009Z,WdiServiceHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Tue Jul 14 04:49:24
2009Z,WdiSystemHost,@%systemroot%\system32\wdi.dll;-500,%SystemRoot%\System32\svchos
t.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:24 2009Z,WdiSystemHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Tue Jul 14 04:49:23 2009Z,EapHost\Parameters,,%SystemRoot%\System32\eapsvc.dll,,,
Tue Jul 14 04:49:20 2009Z,gpsvc\Parameters,,%SystemRoot%\System32\gpsvc.dll,,,
Tue Jul 14 04:49:20 2009Z,NlaSvc\Parameters,,%SystemRoot%\System32\nlasvc.dll,,,
Tue Jul 14 04:49:18 2009Z,BITS\Parameters,,%SystemRoot%\System32\qmgr.dll,,,
Tue Jul 14 04:49:08 2009Z,nsi\Parameters,,%systemroot%\system32\nsisvc.dll,,,
Tue Jul 14 04:49:01 2009Z,.NET CLR Data,,,,,
Tue Jul 14 04:49:01 2009Z,.NET CLR Networking,,,,,
Tue Jul 14 04:49:01 2009Z,.NET Data Provider for Oracle,,,,,
Tue Jul 14 04:49:01 2009Z,.NET Data Provider for SqlServer,,,,,
Tue Jul 14 04:49:01 2009Z,.NETFramework,,,,,
Tue Jul 14 04:49:01 2009Z,adsisvc,,,,,
Tue Jul 14 04:49:01
2009Z,AeLookupSvc,@%SystemRoot%\system32\aelupsvc.dll;-1,%systemroot%\system32\svcho
st.exe -k netsvcs,Share_Process,Manual,localSystem
Tue Jul 14 04:49:01

```

## SYSTEM OUTPUT

2009Z,AeLookupSvc\Parameters,,%SystemRoot%\System32\aelupsvc.dll,,,  
Tue Jul 14 04:49:01  
2009Z,ALG,@%SystemRoot%\system32\Alg.exe;-112,%SystemRoot%\System32\alg.exe,Own\_Proc  
ess,Manual,NT AUTHORITY\LocalService  
Tue Jul 14 04:49:01  
2009Z,AppID,@%systemroot%\system32\appidsvc.dll;-102,\SystemRoot\system32\drivers\ap  
pid.sys,Kernel driver,Manual,  
Tue Jul 14 04:49:01  
2009Z,AppIDSvc,@%systemroot%\system32\appidsvc.dll;-100,%SystemRoot%\system32\svchos  
t.exe -k LocalServiceAndNoImpersonation,Share\_Process,Manual,NT  
Authority\LocalService  
Tue Jul 14 04:49:01 2009Z,AppIDSvc\Parameters,,%SystemRoot%\System32\appidsvc.dll,,,  
Tue Jul 14 04:49:01  
2009Z,Appinfo,@%systemroot%\system32\appinfo.dll;-100,%SystemRoot%\system32\svchos  
t.exe -k netsvcs,Share\_Process,Manual,LocalSystem  
Tue Jul 14 04:49:01 2009Z,Appinfo\Parameters,,%SystemRoot%\System32\appinfo.dll,,,  
Tue Jul 14 04:49:01  
2009Z,AudioEndpointBuilder,@%SystemRoot%\system32\audiosrv.dll;-204,%SystemRoot%\Sys  
tem32\svchost.exe -k LocalSystemNetworkRestricted,Share\_Process,Auto  
Start,LocalSystem  
Tue Jul 14 04:49:01  
2009Z,AudioEndpointBuilder\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,  
Tue Jul 14 04:49:01  
2009Z,AudioSrv,@%SystemRoot%\system32\audiosrv.dll;-200,%SystemRoot%\System32\svchos  
t.exe -k LocalServiceNetworkRestricted,Share\_Process,Auto Start,NT  
AUTHORITY\LocalService  
Tue Jul 14 04:49:01 2009Z,AudioSrv\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,  
Tue Jul 14 04:49:01  
2009Z,AxInstSV,@%SystemRoot%\system32\AxInstSV.dll;-103,%SystemRoot%\system32\svchos  
t.exe -k AxInstSVGroup,Share\_Process,Manual,LocalSystem  
Tue Jul 14 04:49:01 2009Z,AxInstSV\Parameters,,%SystemRoot%\System32\AxInstSV.dll,,,  
Tue Jul 14 04:49:01 2009Z,BattC,,,,,  
Tue Jul 14 04:49:01  
2009Z,BDESVC,@%SystemRoot%\system32\bdesvc.dll;-100,%SystemRoot%\System32\svchost.ex  
e -k netsvcs,Share\_Process,Manual,localSystem  
Tue Jul 14 04:49:01  
2009Z,BFE,@%SystemRoot%\system32\bfe.dll;-1001,%systemroot%\system32\svchost.exe -k  
LocalServiceNoNetwork,Share\_Process,Auto Start,NT AUTHORITY\LocalService  
Tue Jul 14 04:49:01 2009Z,BFE\Parameters,,%SystemRoot%\System32\bfe.dll,,,  
Tue Jul 14 04:49:01  
2009Z,Browser,@%systemroot%\system32\browser.dll;-100,%SystemRoot%\System32\svchost.  
exe -k netsvcs,Share\_Process,Manual,LocalSystem  
Tue Jul 14 04:49:01 2009Z,Browser\Parameters,,%SystemRoot%\System32\browser.dll,,,  
Tue Jul 14 04:49:01 2009Z,Brserid,Brother MFC Serial Port Interface Driver  
(WDM),\SystemRoot\System32\Drivers\Brserid.sys,Kernel driver,Manual,  
Tue Jul 14 04:49:01 2009Z,BrSerWdm,Brother WDM Serial  
driver,\SystemRoot\System32\Drivers\BrSerWdm.sys,Kernel driver,Manual,  
Tue Jul 14 04:49:01 2009Z,BrUsbMdm,Brother MFC USB Fax Only

## SYSTEM OUTPUT

```

Modem,\SystemRoot\System32\Drivers\BrUsbMdm.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01 2009Z,BrUsbSer,Brother MFC USB Serial WDM
Driver,\SystemRoot\System32\Drivers\BrUsbSer.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01
2009Z,bthserv,@%SystemRoot%\System32\bthserv.dll;-101,%SystemRoot%\system32\svchost.
exe -k bthsvcs,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,bthserv\Parameters,,%SystemRoot%\system32\bthserv.dll,,
Tue Jul 14 04:49:01
2009Z,CertPropSvc\Parameters,,%SystemRoot%\System32\certprop.dll,,
Tue Jul 14 04:49:01
2009Z,COMSysApp,@comres.dll;-947,%SystemRoot%\system32\dllhost.exe
/Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235},Own_Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,crypt32,,,,
Tue Jul 14 04:49:01
2009Z,CryptSvc,@%SystemRoot%\system32\cryptsvc.dll;-1001,%SystemRoot%\system32\svcho
st.exe -k NetworkService,Share_Process,Auto Start,NT Authority\NetworkService
Tue Jul 14 04:49:01 2009Z,CryptSvc\Parameters,,%SystemRoot%\system32\cryptsvc.dll,,
Tue Jul 14 04:49:01 2009Z,DCLocator,,,,
Tue Jul 14 04:49:01
2009Z,DcomLaunch,@oleres.dll;-5012,%SystemRoot%\system32\svchost.exe -k
DcomLaunch,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01
2009Z,defragsvc,@%SystemRoot%\system32\defragsvc.dll;-101,%SystemRoot%\system32\svch
ost.exe -k defragsvc,Own_Process,Manual,localSystem
Tue Jul 14 04:49:01
2009Z,dot3svc,@%systemroot%\system32\dot3svc.dll;-1102,%SystemRoot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,localSystem
Tue Jul 14 04:49:01 2009Z,dot3svc\Parameters,,%SystemRoot%\System32\dot3svc.dll,,
Tue Jul 14 04:49:01
2009Z,EFS,@%SystemRoot%\system32\efssvc.dll;-100,%SystemRoot%\System32\lsass.exe,Sha
re_Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,ESENT,,,,
Tue Jul 14 04:49:01
2009Z,EventSystem,@comres.dll;-2450,%SystemRoot%\system32\svchost.exe -k
LocalService,Share_Process,Auto Start,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,EventSystem\Parameters,,%systemroot%\system32\es.dll,,
Tue Jul 14 04:49:01
2009Z,Fax,@%systemroot%\system32\fxsresm.dll;-118,%systemroot%\system32\fxssvc.exe,O
wn_Process,Manual,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,fdPHost,@%systemroot%\system32\fdPHost.dll;-100,%SystemRoot%\system32\svchost.
exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,fdPHost\Parameters,,%SystemRoot%\system32\fdPHost.dll,,
Tue Jul 14 04:49:01 2009Z,FDResPub\Parameters,,%SystemRoot%\system32\fdrespub.dll,,
Tue Jul 14 04:49:01
2009Z,Filetrace,@%SystemRoot%\system32\drivers\filetrace.sys;-10001,system32\drivers
\filetrace.sys,File system driver,Manual,
Tue Jul 14 04:49:01

```

## SYSTEM OUTPUT

2009Z,FontCache3.0.0.0,@%SystemRoot%\system32\PresentationHost.exe;-3309,%systemroot%\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe,Own\_Process,Manual,NT Authority\LocalService  
 Tue Jul 14 04:49:01  
 2009Z,FsDepends,@%SystemRoot%\system32\drivers\fsdepends.sys;-10001,System32\drivers\FsDepends.sys,File system driver,Manual,  
 Tue Jul 14 04:49:01 2009Z,hcw85cir,Hauppauge Consumer Infrared Receiver,\SystemRoot\system32\drivers\hcw85cir.sys,Kernel driver,Manual,  
 Tue Jul 14 04:49:01  
 2009Z,hidserv,@%SystemRoot%\System32\hidserv.dll;-101,%SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted,Share\_Process,Manual,LocalSystem  
 Tue Jul 14 04:49:01 2009Z,hidserv\Parameters,,%SystemRoot%\system32\hidserv.dll,,,  
 Tue Jul 14 04:49:01  
 2009Z,hkmsvc,@%SystemRoot%\system32\kmsvc.dll;-6,%SystemRoot%\System32\svchost.exe -k netsvcs,Share\_Process,Manual,localSystem  
 Tue Jul 14 04:49:01  
 2009Z,HomeGroupListener\Parameters,,%SystemRoot%\system32>ListSvc.dll,,,  
 Tue Jul 14 04:49:01  
 2009Z,HomeGroupProvider,@%SystemRoot%\System32\provsvc.dll;-100,%SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted,Share\_Process,Manual,NT AUTHORITY\LocalService  
 Tue Jul 14 04:49:01  
 2009Z,HomeGroupProvider\Parameters,,%SystemRoot%\system32\provsvc.dll,,,  
 Tue Jul 14 04:49:01 2009Z,idsvc,@%systemroot%\Microsoft.NET\Framework64\v3.0\Windows Communication Foundation\ServiceModelInstallRC.dll;-8193,"%systemroot%\Microsoft.NET\Framework64\v3.0\Windows Communication Foundation\infocard.exe",Share\_Process,Manual,LocalSystem  
 Tue Jul 14 04:49:01 2009Z,IKEEXT\Parameters,,%SystemRoot%\System32\ikeext.dll,,,  
 Tue Jul 14 04:49:01 2009Z,inetaccs,,,,,  
 Tue Jul 14 04:49:01  
 2009Z,IPBusEnum,@%systemroot%\system32\IPBusEnum.dll;-102,%SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted,Share\_Process,Manual,LocalSystem  
 Tue Jul 14 04:49:01  
 2009Z,IPBusEnum\Parameters,,%SystemRoot%\system32\ipbusenum.dll,,,  
 Tue Jul 14 04:49:01  
 2009Z,IpFilterDriver,@%systemroot%\system32\rascfg.dll;-32013,system32\DRIVERS\ipflt drv.sys,Kernel driver,Manual,  
 Tue Jul 14 04:49:01  
 2009Z,iphlpvc,@%SystemRoot%\system32\iphlpvc.dll;-500,%SystemRoot%\System32\svchost.exe -k NetSvc,Share\_Process,Auto Start,LocalSystem  
 Tue Jul 14 04:49:01 2009Z,IPNAT,IP Network Address Translator,System32\drivers\ipnat.sys,Kernel driver,Manual,  
 Tue Jul 14 04:49:01  
 2009Z,IRENUM,@%SystemRoot%\system32\drivers\irenum.sys;-100,system32\drivers\irenum.sys,Kernel driver,Manual,  
 Tue Jul 14 04:49:01  
 2009Z,KeyIso,@keyiso.dll;-100,%SystemRoot%\system32\lsass.exe,Share\_Process,Manual,LocalSystem

## SYSTEM OUTPUT

Tue Jul 14 04:49:01 2009Z,KtmRm,@comres.dll;-2946,%SystemRoot%\System32\svchost.exe  
 -k NetworkServiceAndNoImpersonation,Share\_Process,Manual,NT AUTHORITY\NetworkService  
 Tue Jul 14 04:49:01 2009Z,KtmRm\Parameters,,%systemroot%\system32\msdtckrm.dll,,,  
 Tue Jul 14 04:49:01 2009Z,ldap,,,,,  
 Tue Jul 14 04:49:01  
 2009Z,lltdsvc,@%SystemRoot%\system32\lltdres.dll;-1,%SystemRoot%\System32\svchost.exe  
 -k LocalService,Share\_Process,Manual,NT AUTHORITY\LocalService  
 Tue Jul 14 04:49:01 2009Z,lltdsvc\Parameters,,%SystemRoot%\System32\lltdsvc.dll,,,  
 Tue Jul 14 04:49:01 2009Z,Lsa,,,,,  
 Tue Jul 14 04:49:01  
 2009Z,MMCSS,@%systemroot%\system32\mmcscs.dll;-100,%SystemRoot%\system32\svchost.exe  
 -k netsvcs,Share\_Process,Auto Start,LocalSystem  
 Tue Jul 14 04:49:01 2009Z,MMCSS\Parameters,,%SystemRoot%\system32\mmcscs.dll,,,  
 Tue Jul 14 04:49:01  
 2009Z,MpsSvc,@%SystemRoot%\system32\FirewallAPI.dll;-23090,%SystemRoot%\system32\svchost.exe  
 -k LocalServiceNoNetwork,Share\_Process,Auto Start,NT Authority\LocalService  
 Tue Jul 14 04:49:01 2009Z,MpsSvc\Parameters,,%SystemRoot%\system32\mpssvc.dll,,,  
 Tue Jul 14 04:49:01  
 2009Z,MRxDAV,@%systemroot%\system32\webclnt.dll;-104,\SystemRoot\system32\drivers\mrxdav.sys,  
 File system driver,Manual,  
 Tue Jul 14 04:49:01  
 2009Z,MSDTC,@comres.dll;-2797,%SystemRoot%\System32\msdtc.exe,Own\_Process,Manual,NT  
 AUTHORITY\NetworkService  
 Tue Jul 14 04:49:01  
 2009Z,mshidkmdf,@%SystemRoot%\system32\drivers\mshidkmdf.sys;-100,\SystemRoot\System  
 32\drivers\mshidkmdf.sys,Kernel driver,Manual,  
 Tue Jul 14 04:49:01  
 2009Z,MSiSCSI,@%SystemRoot%\system32\iscsidsc.dll;-5000,%systemroot%\system32\svchos  
 t.exe -k netsvcs,Share\_Process,Manual,LocalSystem  
 Tue Jul 14 04:49:01 2009Z,MSiSCSI\Parameters,,%systemroot%\system32\iscsiexe.dll,,,  
 Tue Jul 14 04:49:01 2009Z,MsRPC,,,Kernel driver,Manual,  
 Tue Jul 14 04:49:01 2009Z,MSSCNTRS,,,,,  
 Tue Jul 14 04:49:01  
 2009Z,napagent,@%SystemRoot%\system32\qagentrt.dll;-6,%SystemRoot%\System32\svchost.  
 exe -k NetworkService,Share\_Process,Manual,NT AUTHORITY\NetworkService  
 Tue Jul 14 04:49:01  
 2009Z,Netlogon,@%SystemRoot%\System32\netlogon.dll;-102,%systemroot%\system32\lsass.  
 exe,Share\_Process,Manual,LocalSystem  
 Tue Jul 14 04:49:01  
 2009Z,Netman,@%SystemRoot%\system32\netman.dll;-109,%SystemRoot%\System32\svchost.exe  
 -k LocalSystemNetworkRestricted,Share\_Process,Manual,LocalSystem  
 Tue Jul 14 04:49:01 2009Z,Netman\Parameters,,%SystemRoot%\System32\netman.dll,,,  
 Tue Jul 14 04:49:01  
 2009Z,netprofm,@%SystemRoot%\system32\netprofm.dll;-202,%SystemRoot%\System32\svchos  
 t.exe -k LocalService,Share\_Process,Manual,NT AUTHORITY\LocalService  
 Tue Jul 14 04:49:01 2009Z,netprofm\Parameters,,%SystemRoot%\System32\netprofm.dll,,,  
 Tue Jul 14 04:49:01  
 2009Z,NlaSvc,@%SystemRoot%\System32\nlasvc.dll;-1,%SystemRoot%\System32\svchost.exe

## SYSTEM OUTPUT

```

-k NetworkService,Share_Process,Auto Start,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,nsi,@%SystemRoot%\system32\nsisvc.dll;-200,%systemroot%\system32\svchost.exe
-k LocalService,Share_Process,Auto Start,NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,NTDS,,,,,
Tue Jul 14 04:49:01
2009Z,p2pimsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8004,%SystemRoot%\System32\svchos
t.exe -k LocalServicePeerNet,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,p2psvc,@%SystemRoot%\system32\p2psvc.dll;-8006,%SystemRoot%\System32\svchost.e
xe -k LocalServicePeerNet,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,PcaSvc,@%SystemRoot%\system32\pcasvc.dll;-1,%systemroot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01 2009Z,PcaSvc\Parameters,,%SystemRoot%\System32\pcasvc.dll,,,
Tue Jul 14 04:49:01 2009Z,PerfDisk,,,,,
Tue Jul 14 04:49:01
2009Z,PerfHost,@%systemroot%\syswow64\perfhost.exe;-2,%SystemRoot%\SysWow64\perfhost
.exe,Own_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,PerfNet,,,,,
Tue Jul 14 04:49:01 2009Z,PerfOS,,,,,
Tue Jul 14 04:49:01 2009Z,PerfProc,,,,,
Tue Jul 14 04:49:01
2009Z,pla,@%systemroot%\system32\pla.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,pla\Parameters,,%systemroot%\system32\pla.dll,,,
Tue Jul 14 04:49:01
2009Z,PlugPlay,@%SystemRoot%\system32\umpnpmgr.dll;-100,%SystemRoot%\system32\svchos
t.exe -k DcomLaunch,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01
2009Z,PNRPAutoReg,@%SystemRoot%\system32\pnrpauto.dll;-8002,%SystemRoot%\System32\sv
chost.exe -k LocalServicePeerNet,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,PNRPsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8000,%SystemRoot%\System32\svchost
.exe -k LocalServicePeerNet,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,PNRPsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,PolicyAgent,@%SystemRoot%\System32\polstore.dll;-5010,%SystemRoot%\system32\sv
chost.exe -k NetworkServiceNetworkRestricted,Share_Process,Manual,NT
Authority\NetworkService
Tue Jul 14 04:49:01
2009Z,PolicyAgent\Parameters,,%SystemRoot%\System32\ipsecsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,PortProxy,,,,,
Tue Jul 14 04:49:01
2009Z,Power,@%SystemRoot%\system32\umpo.dll;-100,%SystemRoot%\system32\svchost.exe
-k DcomLaunch,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01 2009Z,Power\Parameters,,%SystemRoot%\system32\umpo.dll,,,
Tue Jul 14 04:49:01

```

## SYSTEM OUTPUT

2009Z, ProfSvc, @%systemroot%\system32\profsvc.dll; -300, %systemroot%\system32\svchost.exe -k netsvcs, Share\_Process, Auto Start, LocalSystem  
 Tue Jul 14 04:49:01

2009Z, ProtectedStorage, @%systemroot%\system32\psbase.dll; -300, %SystemRoot%\system32\lsass.exe, Share\_Process, Manual, LocalSystem  
 Tue Jul 14 04:49:01

2009Z, QWAVE, @%SystemRoot%\system32\qwave.dll; -1, %windir%\system32\svchost.exe -k LocalServiceAndNoImpersonation, Share\_Process, Manual, NT AUTHORITY\LocalService  
 Tue Jul 14 04:49:01 2009Z, QWAVE\Parameters, , %windir%\system32\qwave.dll, , ,  
 Tue Jul 14 04:49:01

2009Z, QWAVEdrv, @%SystemRoot%\system32\drivers\qwavedrv.sys; -1, \SystemRoot\system32\drivers\qwavedrv.sys, Kernel driver, Manual,  
 Tue Jul 14 04:49:01 2009Z, RasAcid, Remote Access Auto Connection  
 Driver, System32\DRIVERS\rasacd.sys, Kernel driver, Manual,  
 Tue Jul 14 04:49:01 2009Z, RDPDD, , , , ,  
 Tue Jul 14 04:49:01 2009Z, RDPNP, @%systemroot%\system32\drprov.dll; -100, , , ,  
 Tue Jul 14 04:49:01 2009Z, RDPWD, RDP Winstation Driver, , Kernel driver, Manual,  
 Tue Jul 14 04:49:01

2009Z, RemoteRegistry, @regsvc.dll; -1, %SystemRoot%\system32\svchost.exe -k regsvc, Share\_Process, Manual, NT AUTHORITY\LocalService  
 Tue Jul 14 04:49:01

2009Z, RemoteRegistry\Parameters, , %SystemRoot%\system32\regsvc.dll, , ,  
 Tue Jul 14 04:49:01

2009Z, RpcLocator, @%systemroot%\system32\Locator.exe; -2, %SystemRoot%\system32\locator.exe, Own\_Process, Manual, NT AUTHORITY\NetworkService  
 Tue Jul 14 04:49:01 2009Z, RpcSs, @oleres.dll; -5010, %SystemRoot%\system32\svchost.exe -k rpcss, Share\_Process, Auto Start, NT AUTHORITY\NetworkService  
 Tue Jul 14 04:49:01 2009Z, SCardSvr\Parameters, , %SystemRoot%\System32\SCardSvr.dll, , ,  
 Tue Jul 14 04:49:01

2009Z, Schedule, @%SystemRoot%\system32\schedsvc.dll; -100, %systemroot%\system32\svchost.exe -k netsvcs, Share\_Process, Auto Start, LocalSystem  
 Tue Jul 14 04:49:01 2009Z, Schedule\Parameters, , %systemroot%\system32\schedsvc.dll, , ,  
 Tue Jul 14 04:49:01

2009Z, SCPolicySvc, @%SystemRoot%\System32\certprop.dll; -13, %SystemRoot%\system32\svchost.exe -k netsvcs, Share\_Process, Manual, LocalSystem  
 Tue Jul 14 04:49:01

2009Z, SCPolicySvc\Parameters, , %SystemRoot%\System32\certprop.dll, , ,  
 Tue Jul 14 04:49:01

2009Z, SDRSVC, @%SystemRoot%\system32\sdrsvc.dll; -107, %SystemRoot%\system32\svchost.exe -k SDRSVC, Own\_Process, Manual, localSystem  
 Tue Jul 14 04:49:01

2009Z, seclogon, @%SystemRoot%\system32\seclogon.dll; -7001, %windir%\system32\svchost.exe -k netsvcs, Share\_Process, Manual, LocalSystem  
 Tue Jul 14 04:49:01 2009Z, seclogon\Parameters, , %windir%\system32\seclogon.dll, , ,  
 Tue Jul 14 04:49:01

2009Z, SENS, @%SystemRoot%\system32\Sens.dll; -200, %SystemRoot%\system32\svchost.exe -k netsvcs, Share\_Process, Auto Start, LocalSystem  
 Tue Jul 14 04:49:01 2009Z, SENS\Parameters, , %SystemRoot%\System32\sens.dll, , ,

## SYSTEM OUTPUT

```

Tue Jul 14 04:49:01
2009Z,SessionEnv\Parameters,,%SystemRoot%\system32\sessenv.dll,,,
Tue Jul 14 04:49:01
2009Z,ShellHWDetection,@%SystemRoot%\System32\shsvcs.dll;-12288,%SystemRoot%\System32\svchost.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01
2009Z,ShellHWDetection\Parameters,,%SystemRoot%\System32\shsvcs.dll,,,
Tue Jul 14 04:49:01
2009Z,SNMPTRAP,@%SystemRoot%\system32\snmptrap.exe;-3,%SystemRoot%\System32\snmptrap.exe,Own_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,Spooler,@%systemroot%\system32\spoolsv.exe;-1,%SystemRoot%\System32\spoolsv.exe,272,Auto Start,LocalSystem
Tue Jul 14 04:49:01
2009Z,sppsvc,@%SystemRoot%\system32\sppsvc.exe;-101,%SystemRoot%\system32\sppsvc.exe,Own_Process,Auto Start,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,sppuinotify,@%SystemRoot%\system32\sppuinotify.dll;-103,%SystemRoot%\system32\svchost.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,sppuinotify\Parameters,,%SystemRoot%\system32\sppuinotify.dll,,,
Tue Jul 14 04:49:01
2009Z,SSDPSRV,@%systemroot%\system32\ssdpsrv.dll;-100,%SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,SSDPSRV\Parameters,,%SystemRoot%\System32\ssdpsrv.dll,,,
Tue Jul 14 04:49:01
2009Z,SstpSvc,@%SystemRoot%\system32\sstpsvc.dll;-200,%SystemRoot%\system32\svchost.exe -k LocalService,Share_Process,Manual,NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,stisvc\Parameters,,%SystemRoot%\System32\wiaservc.dll,,,
Tue Jul 14 04:49:01
2009Z,swprv,@%SystemRoot%\System32\swprv.dll;-103,%SystemRoot%\System32\svchost.exe -k swprv,Own_Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,swprv\Parameters,,%Systemroot%\System32\swprv.dll,,,
Tue Jul 14 04:49:01 2009Z,SysMain\Parameters,,%systemroot%\system32\sysmain.dll,,,
Tue Jul 14 04:49:01
2009Z,TabletInputService,@%SystemRoot%\system32\TabSvc.dll;-100,%SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01
2009Z,TabletInputService\Parameters,,%SystemRoot%\System32\TabSvc.dll,,,
Tue Jul 14 04:49:01
2009Z,TapiSrv,@%SystemRoot%\system32\tapisrv.dll;-10100,%SystemRoot%\System32\svchost.exe -k NetworkService,Share_Process,Manual,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,TapiSrv\Parameters,,%SystemRoot%\System32\tapisrv.dll,,,
Tue Jul 14 04:49:01 2009Z,TCPIP6TUNNEL,,,,,
Tue Jul 14 04:49:01 2009Z,TCPIPTUNNEL,,,,,
Tue Jul 14 04:49:01 2009Z,TDPIPE,TDPIPE,system32\drivers\tdpipe.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01 2009Z,TDTCP,TDTCP,system32\drivers\tdtcp.sys,Kernel

```



## SYSTEM OUTPUT

```

driver,Manual,
Tue Jul 14 04:49:01
2009Z,TermService,@%SystemRoot%\System32\termsrv.dll;-268,%SystemRoot%\System32\svch
ost.exe -k NetworkService,Share_Process,Manual,NT Authority\NetworkService
Tue Jul 14 04:49:01
2009Z,TermService\Parameters,,%SystemRoot%\System32\termsrv.dll,,,
Tue Jul 14 04:49:01
2009Z,Themes,@%SystemRoot%\System32\themeservice.dll;-8192,%SystemRoot%\System32\svc
host.exe -k netsvcs,Share_Process,Auto Start,LocalSystem
Tue Jul 14 04:49:01
2009Z,Themes\Parameters,,%SystemRoot%\system32\themeservice.dll,,,
Tue Jul 14 04:49:01
2009Z,THREADORDER,@%systemroot%\system32\mmcscs.dll;-102,%SystemRoot%\system32\svchos
t.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,TSDDD,,,,,
Tue Jul 14 04:49:01
2009Z,tssecsrv,@%SystemRoot%\System32\DRIVERS\tssecsrv.sys;-101,system32\DRIVERS\tss
ecsrv.sys,Kernel driver,Manual,
Tue Jul 14 04:49:01 2009Z,UGatherer,,,,,
Tue Jul 14 04:49:01 2009Z,UGTHRSVC,,,,,
Tue Jul 14 04:49:01
2009Z,UI0Detect,@%SystemRoot%\system32\ui0detect.exe;-101,%SystemRoot%\system32\UI0D
etect.exe,272,Manual,LocalSystem
Tue Jul 14 04:49:01
2009Z,upnphost,@%systemroot%\system32\upnphost.dll;-213,%SystemRoot%\system32\svchos
t.exe -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT
AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,upnphost\Parameters,,%SystemRoot%\System32\upnphost.dll,,,
Tue Jul 14 04:49:01
2009Z,UxSms,@%SystemRoot%\system32\dwm.exe;-2000,%SystemRoot%\System32\svchost.exe
-k LocalSystemNetworkRestricted,Share_Process,Auto Start,localSystem
Tue Jul 14 04:49:01 2009Z,UxSms\Parameters,,%SystemRoot%\System32\uxsms.dll,,,
Tue Jul 14 04:49:01
2009Z,VaultSvc,@%SystemRoot%\system32\vaultsvc.dll;-1003,%SystemRoot%\system32\lsass
.exe,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01
2009Z,vds,@%SystemRoot%\system32\vds.exe;-100,%SystemRoot%\System32\vds.exe,Own_Proc
ess,Manual,LocalSystem
Tue Jul 14 04:49:01
2009Z,VSS,@%systemroot%\system32\vssvc.exe;-102,%systemroot%\system32\vssvc.exe,Own_
Process,Manual,LocalSystem
Tue Jul 14 04:49:01 2009Z,W3SVC,,,,,
Tue Jul 14 04:49:01
2009Z,wbengine,@%systemroot%\system32\wbengine.exe;-104,"%systemroot%\system32\wbeng
ine.exe",Own_Process,Manual,localSystem
Tue Jul 14 04:49:01 2009Z,WbioSrv\Parameters,,%SystemRoot%\System32\wbiosrv.dll,,,
Tue Jul 14 04:49:01
2009Z,wcncsvc,@%SystemRoot%\system32\wcncsvc.dll;-3,%SystemRoot%\System32\svchost.ex

```

## SYSTEM OUTPUT

```

e -k LocalServiceAndNoImpersonation,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,wcncsvc\Parameters,,%SystemRoot%\System32\wcncsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,WcsPlugInService,@%SystemRoot%\system32\WcsPlugInService.dll;-200,%SystemRoot%
\system32\svchost.exe -k wcscsvc,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,WcsPlugInService\Parameters,,%SystemRoot%\System32\WcsPlugInService.dll,,,
Tue Jul 14 04:49:01
2009Z,Weccsvc,@%SystemRoot%\system32\weccsvc.dll;-200,%SystemRoot%\system32\svchost.ex
e -k NetworkService,Share_Process,Manual,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,Weccsvc\Parameters,,%SystemRoot%\system32\weccsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,wercplsupport,@%SystemRoot%\System32\wercplsupport.dll;-101,%SystemRoot%\Syste
m32\svchost.exe -k netsvcs,Share_Process,Manual,localSystem
Tue Jul 14 04:49:01
2009Z,wercplsupport\Parameters,,%SystemRoot%\System32\wercplsupport.dll,,,
Tue Jul 14 04:49:01
2009Z,WerSvc,@%SystemRoot%\System32\wersvc.dll;-100,%SystemRoot%\System32\svchost.ex
e -k WerSvcGroup,Share_Process,Manual,localSystem
Tue Jul 14 04:49:01 2009Z,WinDefend\Parameters,,%ProgramFiles%\Windows
Defender\mpsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,WinHttpAutoProxySvc,@%SystemRoot%\system32\winhttp.dll;-100,%SystemRoot%\syste
m32\svchost.exe -k LocalService,Share_Process,Manual,NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,WinRM,@%Systemroot%\system32\wsmsvc.dll;-101,%SystemRoot%\System32\svchost.exe
-k NetworkService,Share_Process,Manual,NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,WinRM\Parameters,,%SystemRoot%\system32\WsmSvc.dll,,,
Tue Jul 14 04:49:01 2009Z,WinSock2,,,,,
Tue Jul 14 04:49:01
2009Z,WPCSvc,@%SystemRoot%\system32\wpcsvc.dll;-100,%SystemRoot%\system32\svchost.ex
e -k LocalServiceNetworkRestricted,Share_Process,Manual,NT Authority\LocalService
Tue Jul 14 04:49:01
2009Z,WPDBusEnum,@%SystemRoot%\system32\wpdbusenum.dll;-100,%SystemRoot%\system32\sv
chost.exe -k LocalSystemNetworkRestricted,Share_Process,Manual,LocalSystem
Tue Jul 14 04:49:01
2009Z,WPDBusEnum\Parameters,,%SystemRoot%\system32\wpdbusenum.dll,,,
Tue Jul 14 04:49:01
2009Z,wscsvc,@%SystemRoot%\System32\wscsvc.dll;-200,%SystemRoot%\System32\svchost.ex
e -k LocalServiceNetworkRestricted,Share_Process,Auto Start,NT
AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,wscsvc\Parameters,,%SystemRoot%\System32\wscsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,WSearchIdxPi,,,,,
Tue Jul 14 04:49:01 2009Z,wuauerv\Parameters,,%systemroot%\system32\wuaueng.dll,,,
Tue Jul 14 04:49:01 2009Z,wudfsvc\Parameters,,%SystemRoot%\System32\WUDFSvc.dll,,,
Tue Jul 14 04:49:01
2009Z,WwanSvc,@%SystemRoot%\System32\wwansvc.dll;-257,%SystemRoot%\system32\svchost.
exe -k LocalServiceNoNetwork,Share_Process,Manual,NT Authority\LocalService

```

## SYSTEM OUTPUT

```
Tue Jul 14 04:49:01 2009Z,WwanSvc\Parameters,,,%SystemRoot%\System32\wwansvc.dll,,,
Tue Jul 14 04:49:01 2009Z,xmlprov,,,,,
Tue Jul 14 02:34:41 2009Z,DcomLaunch\Parameters,,,%SystemRoot%\system32\rpcss.dll,,,
Tue Jul 14 02:34:41 2009Z,RpcSs\Parameters,,,%SystemRoot%\system32\rpcss.dll,,,
-----
```

svc\_plus v.20120625

(System) Lists services/drivers in Services key by LastWrite times in a short format with warnings for type mismatches

```
^^^ Indicates non-standard Type
<<<< Indicates Start mismatch for Driver
**** Indicates ObjectName mismatch for Driver
>>>> Indicates Start mismatch for Service
++++ Indicates nonstandard ObjectName for Service.
```

ControlSet001\Services

Lists services/drivers in Services key by LastWrite times in a short format with warnings for type mismatches

```
^^^ Indicates non-standard Type
<<<< Indicates Start mismatch for Driver
**** Indicates ObjectName mismatch for Driver
>>>> Indicates Start mismatch for Service
++++ Indicates nonstandard ObjectName for Service.
```

Wed Apr 20 02:39:31

2016Z,AsyncMac,@%systemroot%\system32\rascfg.dll;-32000,system32\DRIVERS\asynccmac.sys,,Manual,

Wed Apr 20 02:39:13 2016Z,mfeaack,McAfee Inc.

mfeaack,system32\drivers\mfeaack.sys,,Manual,

Wed Apr 20 02:39:13 2016Z,mfencbdc,McAfee Inc.

mfencbdc,system32\DRIVERS\mfencbdc.sys,,Manual,

Wed Apr 20 02:37:21 2016Z,mfefirek,McAfee Inc.

mfefirek,system32\drivers\mfefirek.sys,,Manual,

Wed Apr 20 02:37:20 2016Z,cfwids,McAfee Inc.

cfwids,system32\drivers\cfwids.sys,,Manual,

Wed Apr 20 02:37:04

2016Z,LanmanServer\Parameters,,,%SystemRoot%\system32\srvsvc.dll,,,

Wed Apr 20 02:37:01 2016Z,mfemms,McAfee Service Controller,"C:\Program Files\Common Files\McAfee\SystemCore\mfemms.exe",,Auto Start,\*\*\*\*LocalSystem

Wed Apr 20 02:36:56 2016Z,vwifimp,Microsoft Virtual WiFi Miniport Service,system32\DRIVERS\vwifimp.sys,,Manual,

Wed Apr 20 02:36:49 2016Z,BrSerIb,Brother Serial Interface Driver(WDM),system32\DRIVERS\BrSerIb.sys,,Manual,

Wed Apr 20 02:36:49 2016Z,BrUsbSIb,Brother Serial USB Driver(WDM),system32\DRIVERS\BrUsbSIb.sys,,Manual,

Wed Apr 20 02:36:49 2016Z,BthEnum,Bluetooth Enumerator Service,system32\DRIVERS\BthEnum.sys,,Manual,

Wed Apr 20 02:36:49 2016Z,BthPan,Bluetooth Device (Personal Area Network),system32\DRIVERS\bthpan.sys,,Manual,

## SYSTEM OUTPUT

Wed Apr 20 02:36:49 2016Z,monitor,Microsoft Monitor Class Function Driver  
 Service,system32\DRIVERS\monitor.sys,,Manual,  
 Wed Apr 20 02:36:49 2016Z,mouhid,Mouse HID  
 Driver,system32\DRIVERS\mouhid.sys,,Manual,  
 Wed Apr 20 02:36:49 2016Z,RFCOMM,Bluetooth Device (RFCOMM Protocol  
 TDI),system32\DRIVERS\rfcomm.sys,,Manual,  
 Wed Apr 20 02:36:49 2016Z,usbprint,Microsoft USB PRINTER  
 Class,system32\DRIVERS\usbprint.sys,,Manual,  
 Wed Apr 20 02:36:49 2016Z,usbscan,USB Scanner  
 Driver,system32\DRIVERS\usbscan.sys,,Manual,  
 Wed Apr 20 02:36:48 2016Z,BTHUSB,Bluetooth Radio USB  
 Driver,system32\Drivers\BTHUSB.sys,,Manual,  
 Wed Apr 20 02:36:48 2016Z,HidUsb,Microsoft HID Class  
 Driver,system32\DRIVERS\hidusb.sys,,Manual,  
 Wed Apr 20 02:36:48 2016Z,kbdhid,Keyboard HID  
 Driver,system32\DRIVERS\kbdhid.sys,,Manual,  
 Wed Apr 20 02:36:48  
 2016Z,scfilter,@%SystemRoot%\System32\drivers\scfilter.sys;-11,system32\DRIVERS\scfi  
 lter.sys,,Manual,  
 Wed Apr 20 02:36:48 2016Z,WinUSB,WinUSB Service,system32\DRIVERS\WinUSB.sys,,Manual,  
 Wed Apr 20 02:36:48 2016Z,WUDFRd,,system32\DRIVERS\WUDFRd.sys,,Manual,  
 Wed Apr 20 02:36:46 2016Z,SPUVCbv,SPUVCb Driver  
 Service,system32\Drivers\SPUVCbv\_x64.sys,,Manual,  
 Wed Apr 20 02:36:44 2016Z,usbccgp,Microsoft USB Generic Parent  
 Driver,system32\DRIVERS\usbccgp.sys,,Manual,  
 Wed Apr 20 02:36:42 2016Z,mfeavfk,Mcafee Inc.  
 mfeavfk,system32\drivers\mfeavfk.sys,,Manual,  
 Wed Apr 20 02:36:41 2016Z,AgereSoftModem,Agere Systems Soft  
 Modem,system32\DRIVERS\agrsm64.sys,,Manual,  
 Wed Apr 20 02:36:41 2016Z,HdAudAddService,Microsoft 1.1 UAA Function Driver for High  
 Definition Audio Service,system32\drivers\HdAudio.sys,,Manual,  
 Wed Apr 20 02:36:41 2016Z,IntcDAud,Intel(R) Display  
 Audio,system32\DRIVERS\IntcDAud.sys,,Manual,  
 Wed Apr 20 02:36:41 2016Z,ksthunk,Kernel Streaming  
 Thunks,\SystemRoot\system32\drivers\ksthunk.sys,,Manual,  
 Wed Apr 20 02:36:41 2016Z,Modem,,system32\drivers\modem.sys,,Manual,  
 Wed Apr 20 02:36:41 2016Z,nusb3hub,Renesas Electronics USB 3.0 Hub  
 Driver,\SystemRoot\system32\drivers\nusb3hub.sys,,Manual,  
 Wed Apr 20 02:36:41 2016Z,Parport,Parallel port  
 driver,\SystemRoot\system32\drivers\parport.sys,,Manual,  
 Wed Apr 20 02:36:41 2016Z,usbhub,Microsoft USB Standard Hub  
 Driver,system32\DRIVERS\usbhub.sys,,Manual,  
 Wed Apr 20 02:36:38 2016Z,mssmbios,Microsoft System Management BIOS  
 Driver,\SystemRoot\system32\drivers\mssmbios.sys,,System Start,  
 Wed Apr 20 02:36:34 2016Z,cdrom,CD-ROM Driver,system32\DRIVERS\cdrom.sys,,System  
 Start,  
 Wed Apr 20 02:36:34 2016Z,Disk,Disk Driver,system32\drivers\disk.sys,,Boot Start,  
 Wed Apr 20 02:36:34 2016Z,hpdskflt,HP Filter,system32\drivers\hpdskflt.sys,,Boot

## SYSTEM OUTPUT

```

Start,
Wed Apr 20 02:36:34 2016Z,rdyboost,System32\drivers\rdyboost.sys,,Boot
Start,
Wed Apr 20 02:36:33 2016Z,13940hci,1394 OHCI Compliant Host
Controller,\SystemRoot\drivers\13940hci.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,Accelerometer,HP Mobile Data Protection
Sensor,\SystemRoot\drivers\Accelerometer.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,ACPI,Microsoft ACPI Driver,\System32\drivers\ACPI.sys,,Boot
Start,
Wed Apr 20 02:36:33
2016Z,AFD,@%SystemRoot%\system32\drivers\afd.sys;-1000,\SystemRoot\system32\drivers\
afd.sys,,System Start,
Wed Apr 20 02:36:33 2016Z,amdkgdag,\system32\DRIVERS\atikmdag.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,amdkgmpfd,AMD PCI Root Bus Lower
Filter,\system32\drivers\amdkgmpfd.sys,,Boot Start,
Wed Apr 20 02:36:33 2016Z,atap1,IDE Channel,\system32\drivers\atap1.sys,,Boot Start,
Wed Apr 20 02:36:33 2016Z,Beep,Beep,,,System Start,
Wed Apr 20 02:36:33
2016Z,blbdrive,\SystemRoot\system32\drivers\blbdrive.sys,,System Start,
Wed Apr 20 02:36:33
2016Z,browser,@%SystemRoot%\system32\browser.dll;-102,\system32\DRIVERS\browser.sys,,Ma
nual,
Wed Apr 20 02:36:33 2016Z,cdfs,CD/DVD File System
Reader,\system32\DRIVERS\cdfs.sys,,Disabled,
Wed Apr 20 02:36:33
2016Z,CLFS,@%SystemRoot%\system32\clfs.sys;-100,\system32\CLFS.sys,,Boot Start,
Wed Apr 20 02:36:33 2016Z,Cmbat,Microsoft ACPI Control Method Battery
Driver,\SystemRoot\system32\drivers\Cmbat.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,CNG,\System32\Drivers\cng.sys,,Boot Start,
Wed Apr 20 02:36:33 2016Z,Combatt,Microsoft Composite Battery
Driver,\system32\drivers\combatt.sys,,Boot Start,
Wed Apr 20 02:36:33 2016Z,CompositeBus,Composite Bus Enumerator
Driver,\SystemRoot\system32\drivers\CompositeBus.sys,,Manual,
Wed Apr 20 02:36:33
2016Z,CSC,@%SystemRoot%\system32\cscsvc.dll;-202,\system32\drivers\csc.sys,,System
Start,
Wed Apr 20 02:36:33
2016Z,Dfsc,@%SystemRoot%\system32\drivers\dfsc.sys;-101,\system32\Drivers\dfsc.sys,,S
ystem Start,
Wed Apr 20 02:36:33
2016Z,discache,@%SystemRoot%\system32\drivers\discache.sys;-102,\system32\drivers\dis
cache.sys,,System Start,
Wed Apr 20 02:36:33 2016Z,DXGkrnl,LDM Graphics
Subsystem,\SystemRoot\system32\drivers\dxgkrnl.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,e1cxpress,Intel(R) PRO/1000 PCI Express Network
Connection Driver C,\system32\DRIVERS\e1c62x64.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,exfat,exFAT File System Driver,,Manual,
Wed Apr 20 02:36:33 2016Z,fastfat,FAT12/16/32 File System Driver,,Manual,

```

## SYSTEM OUTPUT

```

Wed Apr 20 02:36:33
2016Z,FileInfo,@%SystemRoot%\system32\drivers\fileinfo.sys;-100,system32\drivers\fileinfo.sys,,Boot Start,
Wed Apr 20 02:36:33
2016Z,FltMgr,@%SystemRoot%\system32\drivers\fltmgr.sys;-10001,system32\drivers\fltmg
r.sys,,Boot Start,
Wed Apr 20 02:36:33 2016Z,Fs_Rec,,,^^^^8,0,
Wed Apr 20 02:36:33
2016Z,fvevol,@%SystemRoot%\system32\drivers\fvevol.sys;-100,System32\DRIVERS\fvevol.
sys,,Boot Start,
Wed Apr 20 02:36:33 2016Z,HDAudBus,Microsoft UAA Bus Driver for High Definition
Audio,\SystemRoot\system32\drivers\HDAudBus.sys,,Manual,
Wed Apr 20 02:36:33
2016Z,HTTP,@%SystemRoot%\system32\drivers\http.sys;-1,system32\drivers\HTTP.sys,,Man
ual,
Wed Apr 20 02:36:33
2016Z,hwpolicy,@%systemroot%\system32\drivers\hwpolicy.sys;-101,System32\drivers\hwp
olicy.sys,,Boot Start,
Wed Apr 20 02:36:33 2016Z,i8042prt,i8042 Keyboard and PS/2 Mouse Port
Driver,\SystemRoot\system32\drivers\i8042prt.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,igfx,,system32\DRIVERS\igdkmd64.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,intelppm,Intel Processor
Driver,system32\DRIVERS\intelppm.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,JMCR,,system32\DRIVERS\jmcr.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,kbdclass,Keyboard Class
Driver,system32\DRIVERS\kbdclass.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,KSecDD,,System32\Drivers\ksecdd.sys,,Boot Start,
Wed Apr 20 02:36:33 2016Z,KSecPkg,,System32\Drivers\ksecpkg.sys,,Boot Start,
Wed Apr 20 02:36:33 2016Z,lltdio,Link-Layer Topology Discovery Mapper I/O
Driver,system32\DRIVERS\lltdio.sys,,<<<<Auto Start,
Wed Apr 20 02:36:33
2016Z,luafv,@%systemroot%\system32\drivers\luafv.sys;-100,\SystemRoot\system32\drive
rs\luafv.sys,,<<<<Auto Start,
Wed Apr 20 02:36:33
2016Z,MBAMProtector,,\??\C:\Windows\system32\drivers\mbam.sys,,Manual,
Wed Apr 20 02:36:33
2016Z,MBAMSwissArmy,MBAMSwissArmy,\??\C:\Windows\system32\drivers\MBAMSwissArmy.sys,
,Manual,
Wed Apr 20 02:36:33
2016Z,MBAMWebAccessControl,,\??\C:\Windows\system32\drivers\mwac.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,MEIx64,Intel(R) Management Engine Interface
,\SystemRoot\system32\drivers\HECIx64.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,mfehidk,McAfee Inc.
mfehidk,system32\drivers\mfehidk.sys,,Boot Start,
Wed Apr 20 02:36:33 2016Z,mfencrk,McAfee Inc.
mfencrk,system32\DRIVERS\mfencrk.sys,,Manual,
Wed Apr 20 02:36:33 2016Z,mfesapsn,McAfee Process Start Notification
Service,\??\C:\Program Files (x86)\McAfee\SiteAdvisor\x64\mfesapsn.sys,,Manual,

```

## SYSTEM OUTPUT

Wed Apr 20 02:36:33 2016Z,mfewfpk,McAfee Inc.  
 mfewfpk,system32\drivers\mfewfpk.sys,,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,mouclass,Mouse Class  
 Driver,system32\DRIVERS\mouclass.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,mountmgr,@%SystemRoot%\system32\drivers\mountmgr.sys;-100,System32\drivers\mountmgr.sys,,Boot Start,  
 Wed Apr 20 02:36:33  
 2016Z,mpsdrv,@%SystemRoot%\system32\FirewallAPI.dll;-23092,system32\drivers\mpsdrv.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,mrxsmb,@%systemroot%\system32\wkssvc.dll;-1002,system32\DRIVERS\mrxsmb.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,mrxsmb10,@%systemroot%\system32\wkssvc.dll;-1004,system32\DRIVERS\mrxsmb10.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,mrxsmb20,@%systemroot%\system32\wkssvc.dll;-1006,system32\DRIVERS\mrxsmb20.sys,,Manual,  
 Wed Apr 20 02:36:33 2016Z,msahci,,system32\drivers\msahci.sys,,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,Msfs,,,,System Start,  
 Wed Apr 20 02:36:33 2016Z,msisadrv,,system32\drivers\msisadrv.sys,,Boot Start,  
 Wed Apr 20 02:36:33  
 2016Z,Mup,@%systemroot%\system32\drivers\mup.sys;-101,system32\Drivers\mup.sys,,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,NativeWifiP,NativeWiFi  
 Filter,system32\DRIVERS\nwifi.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,NDIS,@%SystemRoot%\system32\drivers\ndis.sys;-200,system32\drivers\ndis.sys,,Boot Start,  
 Wed Apr 20 02:36:33  
 2016Z,NdisTapi,@%systemroot%\system32\rascfg.dll;-32001,system32\DRIVERS\ndistapi.sys,,Manual,  
 Wed Apr 20 02:36:33 2016Z,Ndisuio,NDIS Usermode I/O  
 Protocol,system32\DRIVERS\ndisuio.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,Ndiswan,@%systemroot%\system32\rascfg.dll;-32002,system32\DRIVERS\ndiswan.sys,,Manual,  
 Wed Apr 20 02:36:33 2016Z,NDProxy,NDIS Proxy,,Manual,  
 Wed Apr 20 02:36:33 2016Z,NetBIOS,NetBIOS  
 Interface,system32\DRIVERS\netbios.sys,,System Start,  
 Wed Apr 20 02:36:33  
 2016Z,NetBT,@%SystemRoot%\system32\drivers\netbt.sys;-2,system32\DRIVERS\netbt.sys,,System Start,  
 Wed Apr 20 02:36:33 2016Z,NETwNs64,\_\_\_ Intel(R) Wireless WiFi Link 5000 Series  
 Adapter Driver for Windows 7 - 64 Bit,system32\DRIVERS\NETwsw00.sys,,Manual,  
 Wed Apr 20 02:36:33 2016Z,Npfs,,,,System Start,  
 Wed Apr 20 02:36:33

## SYSTEM OUTPUT

2016Z,nsiproxy,@%SystemRoot%\system32\drivers\nsiproxy.sys;-2,system32\drivers\nsiproxy.sys,,System Start,  
 Wed Apr 20 02:36:33 2016Z,Ntfs,,,,Manual,  
 Wed Apr 20 02:36:33 2016Z,Null,,,,System Start,  
 Wed Apr 20 02:36:33 2016Z,nusb3xhc,Renesas Electronics USB 3.0 Host Controller Driver,\SystemRoot\system32\drivers\nusb3xhc.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,partmgr,@%SystemRoot%\system32\drivers\partmgr.sys;-100,system32\drivers\partmgr.sys,,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,pci,PCI Bus Driver,system32\drivers\pci.sys,,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,pcw,Performance Counters for Windows Driver,system32\drivers\pcw.sys,,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,PEAUTH,PEAUTH,system32\drivers\peauth.sys,,<<<<Auto Start,  
 Wed Apr 20 02:36:33  
 2016Z,PptpMiniport,@%systemroot%\system32\rascfg.dll;-32006,system32\DRIVERS\raspptp.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,Psched,@%SystemRoot%\System32\drivers\pacer.sys;-101,system32\DRIVERS\pacer.sys,,System Start,  
 Wed Apr 20 02:36:33 2016Z,RasAgileVpn,WAN Miniport (IKEv2),system32\DRIVERS\AgileVpn.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,Rasl2tp,@%systemroot%\system32\rascfg.dll;-32005,system32\DRIVERS\rasl2tp.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,RasPppoe,@%systemroot%\system32\rascfg.dll;-32007,system32\DRIVERS\raspppoe.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,RasSstp,@%systemroot%\system32\sstpsvc.dll;-202,system32\DRIVERS\rassstp.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,rdbss,@%systemroot%\system32\wkssvc.dll;-1000,system32\DRIVERS\rdbss.sys,,System Start,  
 Wed Apr 20 02:36:33 2016Z,rdpbus,Remote Desktop Device Redirector Bus Driver,\SystemRoot\system32\drivers\rdpbus.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,RDPCDD,@%systemroot%\system32\DRIVERS\RDPCDD.sys;-100,system32\DRIVERS\RDPCDD.sys,,System Start,  
 Wed Apr 20 02:36:33  
 2016Z,RDPENCDD,@%systemroot%\system32\drivers\RDPCDD.sys;-101,system32\drivers\rdpencdd.sys,,System Start,  
 Wed Apr 20 02:36:33  
 2016Z,RDPREFMP,@%systemroot%\system32\drivers\RdpRefMp.sys;-101,system32\drivers\rdprefmp.sys,,System Start,  
 Wed Apr 20 02:36:33 2016Z,rspndr,Link-Layer Topology Discovery Responder,system32\DRIVERS\rspndr.sys,,<<<<Auto Start,  
 Wed Apr 20 02:36:33 2016Z,secdrv,Security Driver,,,Disabled,  
 Wed Apr 20 02:36:33 2016Z,Serenum,Serenum Filter



## SYSTEM OUTPUT

Driver,system32\DRIVERS\serenum.sys,,Manual,  
 Wed Apr 20 02:36:33 2016Z,Serial,Serial port  
 driver,system32\DRIVERS\serial.sys,,System Start,  
 Wed Apr 20 02:36:33 2016Z,spldr,Security Processor Loader Driver,,,Boot Start,  
 Wed Apr 20 02:36:33  
 2016Z,svr,@%systemroot%\system32\svrsvc.dll;-102,System32\DRIVERS\svr.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,svr2,@%systemroot%\system32\svrsvc.dll;-104,System32\DRIVERS\svr2.sys,,Manual,  
 Wed Apr 20 02:36:33 2016Z,svrnet,,System32\DRIVERS\svrnet.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,storflt,@%SystemRoot%\system32\vmstorfltres.dll;-1000,system32\drivers\vmstorfl  
 t.sys,,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,swenum,Software Bus  
 Driver,\SystemRoot\system32\drivers\swenum.sys,,Manual,  
 Wed Apr 20 02:36:33  
 2016Z,Tcpip,@%SystemRoot%\system32\tcpipcfg.dll;-50003,System32\drivers\tcpip.sys,,B  
 oot Start,  
 Wed Apr 20 02:36:33 2016Z,tcpipreg,TCP/IP Registry  
 Compatibility,System32\drivers\tcpipreg.sys,,<<<<Auto Start,  
 Wed Apr 20 02:36:33  
 2016Z,tdx,@%SystemRoot%\system32\tcpipcfg.dll;-50004,system32\DRIVERS\tdx.sys,,Syste  
 m Start,  
 Wed Apr 20 02:36:33 2016Z,TermDD,Terminal Device  
 Driver,\SystemRoot\system32\drivers\termdd.sys,,System Start,  
 Wed Apr 20 02:36:33 2016Z,TPM,TPM,system32\drivers\tpm.sys,,Manual,  
 Wed Apr 20 02:36:33 2016Z,tunnel,Microsoft Tunnel Miniport Adapter  
 Driver,system32\DRIVERS\tunnel.sys,,Manual,  
 Wed Apr 20 02:36:33 2016Z,udfs,udfs,system32\DRIVERS\udfs.sys,,Disabled,  
 Wed Apr 20 02:36:33 2016Z,umbus,UMBus Enumerator  
 Driver,\SystemRoot\system32\drivers\umbus.sys,,Manual,  
 Wed Apr 20 02:36:33 2016Z,usbhci,Microsoft USB 2.0 Enhanced Host Controller  
 Miniport Driver,\SystemRoot\system32\drivers\usbhci.sys,,Manual,  
 Wed Apr 20 02:36:33 2016Z,vdrvroot,Microsoft Virtual Drive Enumerator  
 Driver,system32\drivers\vdrvroot.sys,,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,VgaSave,,\SystemRoot\System32\drivers\vga.sys,,System  
 Start,  
 Wed Apr 20 02:36:33 2016Z,volmgr,Volume Manager  
 Driver,system32\drivers\volmgr.sys,,Boot Start,  
 Wed Apr 20 02:36:33  
 2016Z,volmgrx,@%SystemRoot%\system32\drivers\volmgrx.sys;-100,System32\drivers\volmg  
 rx.sys,,Boot Start,  
 Wed Apr 20 02:36:33 2016Z,volsnap,Storage volumes,system32\drivers\volsnap.sys,,Boot  
 Start,  
 Wed Apr 20 02:36:33 2016Z,vwifibus,Virtual WiFi Bus  
 Driver,system32\DRIVERS\vwifibus.sys,,Manual,  
 Wed Apr 20 02:36:33 2016Z,vwifflt,Virtual WiFi Filter  
 Driver,system32\DRIVERS\vwifflt.sys,,System Start,  
 Wed Apr 20 02:36:33

## SYSTEM OUTPUT

2016Z,Wanarpv6,@%systemroot%\system32\rascfg.dll;-32012,system32\DRIVERS\wanarp.sys,  
, System Start,  
Wed Apr 20 02:36:33  
2016Z,Wdf01000,@%SystemRoot%\system32\drivers\Wdf01000.sys;-1000,system32\drivers\Wd  
f01000.sys,, Boot Start,  
Wed Apr 20 02:36:33 2016Z,WfpLwf,WFP Lightweight  
Filter,system32\DRIVERS\wfplwf.sys,, System Start,  
Wed Apr 20 02:36:33 2016Z,WIMMount,WIMMount,system32\drivers\wimmount.sys,, Manual,  
Wed Apr 20 02:36:33 2016Z,WmiAcpi,Microsoft Windows Management Interface for  
ACPI,\SystemRoot\system32\drivers\wmiaapi.sys,, Manual,  
Wed Apr 20 02:36:33 2016Z,ws2ifsl,Windows Socket 2.0 Non-IFS Service Provider  
Support Environment,\SystemRoot\system32\drivers\ws2ifsl.sys,, System Start,  
Wed Apr 20 02:36:33  
2016Z,WudFPf,@%SystemRoot%\system32\drivers\Wudfpf.sys;-1000,system32\drivers\WudFPf  
.sys,, Manual,  
Tue Apr 19 01:25:12 2016Z,MSK80Service,McAfee Anti-Spam Service,"C:\Program  
Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,, Auto  
Start,\*\*\*\*LocalSystem  
Tue Apr 19 01:25:10 2016Z,McProxy,McAfee Proxy Service,"C:\Program Files\Common  
Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,, Auto Start,\*\*\*\*LocalSystem  
Tue Apr 19 01:25:09 2016Z,McNaiAnn,McAfee VirusScan Announcer,"C:\Program  
Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,, Auto  
Start,\*\*\*\*LocalSystem  
Tue Apr 19 01:25:08 2016Z,McMPFSvc,McAfee Personal Firewall Service,"C:\Program  
Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,, Auto  
Start,\*\*\*\*LocalSystem  
Tue Apr 19 01:25:06 2016Z,McBootDelayStartSvc,McAfee Boot Delay Start  
Service,"C:\Program Files\Common Files\McAfee\Platform\McSvcHost\McSvHost.exe"  
/McCoreSvc,, Auto Start,\*\*\*\*LocalSystem  
Tue Apr 19 01:25:05 2016Z,HomeNetSvc,McAfee Home Network,"C:\Program Files\Common  
Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,, Auto Start,\*\*\*\*LocalSystem  
Tue Apr 19 01:25:04 2016Z,McAPExe,McAfee AP Service,"C:\Program  
Files\McAfee\MS\McAPExe.exe",, Auto Start,\*\*\*\*LocalSystem  
Tue Apr 19 01:25:03 2016Z,mfefire,McAfee Firewall Core Service,"C:\Program  
Files\Common Files\McAfee\SystemCore\mfefire.exe",, Manual,\*\*\*\*LocalSystem  
Tue Apr 19 01:25:00 2016Z,mfevtp,McAfee Validation Trust Protection  
Service,"C:\Windows\system32\mfevtps.exe",, Manual,\*\*\*\*LocalSystem  
Tue Apr 19 01:22:11 2016Z,McAfee SiteAdvisor Service,McAfee SiteAdvisor  
Service,"C:\Program Files (x86)\McAfee\SiteAdvisor\McSACore.exe",, Auto  
Start,\*\*\*\*LocalSystem  
Tue Apr 19 01:21:52 2016Z,mcpltsvc,McAfee Platform Services,"C:\Program Files\Common  
Files\McAfee\Platform\McSvcHost\McSvHost.exe" /McCoreSvc,, Auto Start,\*\*\*\*LocalSystem  
Tue Apr 19 01:21:37 2016Z,PEFService,Intel Security PEF Service,"C:\Program  
Files\Common Files\Intel Security\PEF\CORE\PEFService.exe",, Auto  
Start,\*\*\*\*LocalSystem  
Tue Apr 19 01:21:20 2016Z,mccspsvc,McAfee CSP Service,"C:\Program Files\Common  
Files\McAfee\CSP\1.8.267.0\McCSPServiceHost.exe",, Auto Start,\*\*\*\*LocalSystem  
Sat Apr 16 22:47:57 2016Z,MSPQM,Microsoft Streaming Quality Manager

## SYSTEM OUTPUT

Proxy,system32\drivers\MSPQM.sys,,Manual,  
 Wed Apr 13 11:43:26  
 2016Z,TrustedInstaller,@%SystemRoot%\servicing\TrustedInstaller.exe;-100,%SystemRoot%\servicing\TrustedInstaller.exe,,Manual,\*\*\*\*LocalSystem  
 Wed Apr 13 11:42:56 2016Z,PlugPlay\Parameters,,%SystemRoot%\system32\umpnpmgr.dll,,  
 Wed Apr 6 14:20:46 2016Z,USBSTOR,USB Mass Storage  
 Driver,system32\DRIVERS\USBSTOR.SYS,,Manual,  
 Wed Apr 6 00:30:11  
 2016Z,Winmgmt\Parameters,,%SystemRoot%\system32\wbem\WMIsvc.dll,,  
 Sun Mar 27 00:31:42 2016Z,MBAMScheduler,, "C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamscheduler.exe",,Auto Start,\*\*\*\*LocalSystem  
 Sun Mar 27 00:31:41 2016Z,MBAMService,, "C:\Program Files (x86)\Malwarebytes Anti-Malware\mbamservice.exe",,Auto Start,\*\*\*\*LocalSystem  
 Thu Mar 10 19:38:21 2016Z,Netaapl,Apple Mobile Device Ethernet Service,system32\DRIVERS\netaapl64.sys,,Manual,  
 Thu Mar 10 19:38:21 2016Z,USBAAPL64,Apple Mobile USB Driver,system32\Drivers\usbaapl64.sys,,Manual,  
 Thu Feb 25 02:16:29 2016Z,usbaudio,USB Audio Driver (WDM),system32\drivers\usbaudio.sys,,Manual,  
 Sun Feb 21 00:01:18 2016Z,WinDefend,@%ProgramFiles%\Windows Defender\MsMpRes.dll;-103,%SystemRoot%\System32\svchost.exe -k secsvcs,,Manual,\*\*\*\*LocalSystem  
 Sun Feb 14 15:57:33 2016Z,drmkaud,Microsoft Trusted Audio Drivers,\SystemRoot\system32\drivers\drmkaud.sys,,Manual,  
 Sun Feb 14 15:57:33 2016Z,MSKSSRV,Microsoft Streaming Service Proxy,system32\drivers\MSKSSRV.sys,,Manual,  
 Sun Feb 14 15:57:33 2016Z,MSPCLOCK,Microsoft Streaming Clock Proxy,system32\drivers\MSPCLOCK.sys,,Manual,  
 Sun Feb 14 15:57:33 2016Z,MSTEE,Microsoft Streaming Tee/Sink-to-Sink Converter,system32\drivers\MSTEE.sys,,Manual,  
 Wed Feb 10 01:34:39 2016Z,tap0901,TAP-Windows Adapter V9,system32\DRIVERS\tap0901.sys,,Manual,  
 Tue Feb 9 22:07:39 2016Z,clr\_optimization\_v2.0.50727\_32,Microsoft .NET Framework NGEN v2.0.50727\_X86,%systemroot%\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe,,Disabled,\*\*\*\*LocalSystem  
 Tue Feb 9 22:07:39 2016Z,clr\_optimization\_v2.0.50727\_64,Microsoft .NET Framework NGEN v2.0.50727\_X64,%systemroot%\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe,,Disabled,\*\*\*\*LocalSystem  
 Wed Feb 3 04:32:57  
 2016Z,BITS,@%SystemRoot%\system32\qmgr.dll;-1000,%SystemRoot%\System32\svchost.exe -k netsvcs,,Auto Start,\*\*\*\*LocalSystem  
 Tue Feb 2 00:31:05 2016Z,BrYNSvc,BrYNSvc, "C:\Program Files (x86)\Browny02\BrYNSvc.exe",,Manual,\*\*\*\*LocalSystem  
 Tue Feb 2 00:20:01 2016Z,PDFProFiltSrvPP,PDFProFiltSrvPP,C:\Program Files (x86)\Nuance\PaperPort\PDFProFiltSrvPP.exe,,Auto Start,\*\*\*\*LocalSystem  
 Mon Feb 1 03:04:18 2016Z,StillCam,Still Serial Digital Camera

## SYSTEM OUTPUT

Driver,system32\DRIVERS\serscan.sys,,Manual,  
Tue Jan 19 22:34:35 2016Z,IntuitUpdateServiceV4,Intuit Update Service v4,"C:\Program Files (x86)\Common Files\Intuit\Update Service v4\IntuitUpdateService.exe",,Auto Start,\*\*\*\*LocalSystem  
Tue Jan 19 22:14:22  
2016Z,msiserver,@%SystemRoot%\system32\msimg.dll;-27,%systemroot%\system32\msiexec.exe /V,,Auto Start,\*\*\*\*LocalSystem  
Thu Jan 7 22:15:30 2016Z,iPod Service,iPod Service,"C:\Program Files\iPod\bin\iPodService.exe",,Manual,\*\*\*\*LocalSystem  
Thu Jan 7 22:11:07 2016Z,Bonjour Service,Bonjour Service,"C:\Program Files\Bonjour\mDNSResponder.exe",,Auto Start,\*\*\*\*LocalSystem  
Fri Jan 1 20:52:19 2016Z,MozillaMaintenance,Mozilla Maintenance Service,"C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe",,Manual,\*\*\*\*LocalSystem  
Sat Nov 28 20:21:16 2015Z,{1BDD94C3-9D85-46F0-87E3-BD3288A5F6BD},,,^ ^ ^ ^,,  
Wed Nov 11 20:32:01  
2015Z,SharedAccess\Parameters,,%SystemRoot%\System32\ipnathlp.dll,,  
Wed Nov 11 20:31:53  
2015Z,SharedAccess,@%SystemRoot%\system32\ipnathlp.dll;-106,%SystemRoot%\System32\svchost.exe -k netsvcs,,Manual,\*\*\*\*LocalSystem  
Wed Nov 11 20:31:50 2015Z,{A9E50A43-973B-4CAD-B78E-EA0321A4A293},,,^ ^ ^ ^,,  
Mon Oct 19 23:21:21 2015Z,MSDTC Bridge 4.0.0.0,,^ ^ ^ ^,,  
Mon Oct 19 23:21:21 2015Z,SMSSvcHost 4.0.0.0,,^ ^ ^ ^,,  
Mon Oct 19 23:21:21 2015Z,Windows Workflow Foundation 4.0.0.0,,^ ^ ^ ^,,  
Fri Oct 2 14:28:51 2015Z,McODS,McAfee Scanner,"C:\Program Files\McAfee\VirusScan\mcods.exe",,Manual,\*\*\*\*LocalSystem  
Wed Sep 23 03:20:38 2015Z,usbvideo,USB Video Device (WDM),System32\Drivers\usbvideo.sys,,Manual,  
Sat Sep 12 00:14:59 2015Z,ASP.NET,,^ ^ ^ ^,,  
Sat Sep 12 00:14:57 2015Z,ASP.NET\_4.0.30319,,^ ^ ^ ^,,  
Sat Sep 12 00:14:57 2015Z,aspnet\_state,ASP.NET State Service,%SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\aspnet\_state.exe,,Disabled,\*\*\*\*NT AUTHORITY\NetworkService  
Sat Sep 12 00:14:30  
2015Z,NetMsmqActivator,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModel\InstallRC.dll;-8195,"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSSvcHost.exe" -NetMsmqActivator,,Disabled,\*\*\*\*NT AUTHORITY\NetworkService  
Sat Sep 12 00:14:29  
2015Z,NetPipeActivator,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModel\InstallRC.dll;-8197,C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSSvcHost.exe,,Disabled,\*\*\*\*NT AUTHORITY\LocalService  
Sat Sep 12 00:14:25  
2015Z,NetTcpActivator,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModel\InstallRC.dll;-8199,C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSSvcHost.exe,,Disabled,\*\*\*\*NT AUTHORITY\LocalService  
Sat Sep 12 00:14:23  
2015Z,NetTcpPortSharing,@C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ServiceModel\InstallRC.dll;-8201,C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSSvcHost.exe,

## SYSTEM OUTPUT

,Disabled,\*\*\*\*NT AUTHORITY\LocalService  
Sat Sep 12 00:14:19 2015Z,.NET Memory Cache 4.0,,,^ ^ ^ ^,,  
Sat Sep 12 00:09:28  
2015Z,stisvc,@%SystemRoot%\system32\wiaservc.dll;-9,%SystemRoot%\system32\svchost.exe -k imgsvc,,Auto Start,\*\*\*\*NT AUTHORITY\LocalService  
Fri Sep 11 18:30:16 2015Z,Apple Mobile Device,,,^ ^ ^ ^,,  
Fri Sep 11 17:57:59 2015Z,Apple Mobile Device Service,Apple Mobile Device Service,"C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe",,Auto Start,\*\*\*\*LocalSystem  
Fri Sep 11 14:56:27 2015Z,gupdate,Google Update Service (gupdate),"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /svc,,Auto Start,\*\*\*\*LocalSystem  
Fri Sep 11 14:56:27 2015Z,gupdatem,Google Update Service (gupdatem),"C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /medsvc,,Manual,\*\*\*\*LocalSystem  
Fri Sep 11 07:47:27  
2015Z,WbioSrv,@%systemroot%\system32\wbiosrv.dll;-100,%SystemRoot%\system32\svchost.exe -k WbioSvcGroup,,Manual,\*\*\*\*LocalSystem  
Thu Sep 10 21:49:02 2015Z,clr\_optimization\_v4.0.30319\_64,Microsoft .NET Framework NGEN v4.0.30319\_X64,C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe,,Auto Start,\*\*\*\*LocalSystem  
Thu Sep 10 21:49:01 2015Z,clr\_optimization\_v4.0.30319\_32,Microsoft .NET Framework NGEN v4.0.30319\_X86,C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe,,Auto Start,\*\*\*\*LocalSystem  
Thu Sep 10 21:48:06 2015Z,.NET CLR Networking 4.0.0.0,,,^ ^ ^ ^,,  
Thu Sep 10 21:30:14  
2015Z,eventlog,@%SystemRoot%\system32\eventlog.dll;-200,%SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted,,Auto Start,\*\*\*\*NT AUTHORITY\LocalService  
Thu Sep 10 21:30:14 2015Z,Outlook,,,^ ^ ^ ^,,  
Thu Sep 10 21:28:37 2015Z,osppsvc,Office Software Protection Platform,"C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE",,Manual,\*\*\*\*NT AUTHORITY\NetworkService  
Thu Sep 10 20:46:43  
2015Z,DiagTrack,@%SystemRoot%\system32\UtcResources.dll;-3001,%SystemRoot%\System32\svchost.exe -k utcsvc,,Auto Start,\*\*\*\*LocalSystem  
Thu Sep 10 20:46:43  
2015Z,DiagTrack\Parameters,,%SystemRoot%\system32\diagtrack.dll,,  
Thu Sep 10 19:42:05 2015Z,ose,Office Source Engine,"C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE",,Manual,\*\*\*\*LocalSystem  
Thu Sep 10 17:10:15  
2015Z,IKEEXT,@%SystemRoot%\system32\ikeext.dll;-501,%systemroot%\system32\svchost.exe -k netsvcs,,Auto Start,\*\*\*\*LocalSystem  
Thu Sep 10 17:09:34 2015Z,HipShieldK,McAfee Inc.  
HipShieldK,system32\drivers\HipShieldK.sys,,Manual,  
Thu Sep 10 16:33:32 2015Z,odserv,Microsoft Office Diagnostics Service,"C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\ODSERV.EXE",,Manual,\*\*\*\*LocalSystem  
Thu Sep 10 04:09:03 2015Z,WMPNetworkSvc,@%PROGRAMFILES%\Windows Media

## SYSTEM OUTPUT

Player\wmpnetwk.exe;-101,"%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe",,Auto Start,\*\*\*\*NT AUTHORITY\NetworkService

Thu Sep 10 04:09:02

2015Z,HomeGroupListener,@%SystemRoot%\System32\ListSvc.dll;-100,%SystemRoot%\System32\svchost.exe -k LocalSystemNetworkRestricted,,Manual,\*\*\*\*LocalSystem

Thu Sep 10 04:08:46

2015Z,FDResPub,@%systemroot%\system32\fdrespub.dll;-100,%SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation,,Auto Start,\*\*\*\*NT AUTHORITY\LocalService

Thu Sep 3 18:12:30

2015Z,WSearch,@%systemroot%\system32\SearchIndexer.exe;-103,%systemroot%\system32\SearchIndexer.exe /Embedding,,Auto Start,\*\*\*\*LocalSystem

Thu Sep 3 17:49:58

2015Z,CertPropSvc,@%SystemRoot%\System32\certprop.dll;-11,%SystemRoot%\system32\svchost.exe -k netsvcs,,Auto Start,\*\*\*\*LocalSystem

Thu Sep 3 17:49:58

2015Z,SCardSvr,@%SystemRoot%\System32\SCardSvr.dll;-1,%SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation,,Auto Start,\*\*\*\*NT AUTHORITY\LocalService

Thu Sep 3 17:49:37 2015Z,{720B974A-3E6B-42BF-9839-4EE6CD676477},,,^^^^,,

Fri Feb 20 18:42:20 2015Z,adp94xx,,\SystemRoot\system32\drivers\adp94xx.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,adpahci,,\SystemRoot\system32\drivers\adpahci.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,adpu320,,\SystemRoot\system32\drivers\adpu320.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,aliide,,\SystemRoot\system32\drivers\aliide.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,amdide,,\SystemRoot\system32\drivers\amdide.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,amdsata,,\SystemRoot\system32\drivers\amdsata.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,amdsbs,,\SystemRoot\system32\drivers\amdsbs.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,arc,,\SystemRoot\system32\drivers\arc.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,arcsas,,\SystemRoot\system32\drivers\arcsas.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,cmdide,,\SystemRoot\system32\drivers\cmdide.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,elxstor,,\SystemRoot\system32\drivers\elxstor.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,HpSAMD,,\SystemRoot\system32\drivers\HpSAMD.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,iaStorV,,\SystemRoot\system32\drivers\iaStorV.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,iirsp,,\SystemRoot\system32\drivers\iirsp.sys,,Manual,

Fri Feb 20 18:42:20

2015Z,intelide,,\SystemRoot\system32\drivers\intelide.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,isapnp,,\SystemRoot\system32\drivers\isapnp.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,LSI\_FC,,\SystemRoot\system32\drivers\lsi\_fc.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,LSI\_SAS,,\SystemRoot\system32\drivers\lsi\_sas.sys,,Manual,

Fri Feb 20 18:42:20

2015Z,LSI\_SAS2,,\SystemRoot\system32\drivers\lsi\_sas2.sys,,Manual,

Fri Feb 20 18:42:20

2015Z,LSI\_SCSI,,\SystemRoot\system32\drivers\lsi\_scsi.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,megasas,,\SystemRoot\system32\drivers\megasas.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,MegaSR,,\SystemRoot\system32\drivers\MegaSR.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,mpio,,\SystemRoot\system32\drivers\mpio.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,msdsm,,\SystemRoot\system32\drivers\msdsm.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,nfrd960,,\SystemRoot\system32\drivers\nfrd960.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,nvraid,,\SystemRoot\system32\drivers\nvraid.sys,,Manual,

Fri Feb 20 18:42:20 2015Z,nvstor,,\SystemRoot\system32\drivers\nvstor.sys,,Manual,

## SYSTEM OUTPUT

```

Fri Feb 20 18:42:20 2015Z,pciide,,\SystemRoot\system32\drivers\pciide.sys,,Manual,
Fri Feb 20 18:42:20 2015Z,ql2300,,\SystemRoot\system32\drivers\ql2300.sys,,Manual,
Fri Feb 20 18:42:20 2015Z,ql40xx,,\SystemRoot\system32\drivers\ql40xx.sys,,Manual,
Fri Feb 20 18:42:20
2015Z,sbp2port,,\SystemRoot\system32\drivers\sbp2port.sys,,Manual,
Fri Feb 20 18:42:20
2015Z,SiSRaid2,,\SystemRoot\system32\drivers\SiSRaid2.sys,,Manual,
Fri Feb 20 18:42:20
2015Z,SiSRaid4,,\SystemRoot\system32\drivers\sisraid4.sys,,Manual,
Fri Feb 20 18:42:20
2015Z,stexstor,,\SystemRoot\system32\drivers\stexstor.sys,,Manual,
Fri Feb 20 18:42:20 2015Z,storvsc,,\SystemRoot\system32\drivers\storvsc.sys,,Manual,
Fri Feb 20 18:42:20 2015Z,viaide,,\SystemRoot\system32\drivers\viaide.sys,,Manual,
Fri Feb 20 18:42:20 2015Z,vmbus,,\SystemRoot\system32\drivers\vmbus.sys,,Manual,
Fri Feb 20 18:42:20 2015Z,vsmraid,,\SystemRoot\system32\drivers\vsmraid.sys,,Manual,
Fri Feb 20 18:42:20 2015Z,Wd,,\SystemRoot\system32\drivers\wd.sys,,Manual,
Fri Feb 20 18:42:17
2015Z,EapHost,@%systemroot%\system32\eapsvc.dll;-1,%SystemRoot%\System32\svchost.exe
-k netsvcs,,Manual,****localSystem
Fri Feb 20 18:42:17 2015Z,terminpt,Microsoft Remote Desktop Input
Driver,\SystemRoot\system32\drivers\terminpt.sys,,Manual,
Fri Feb 20 18:42:17 2015Z,TsUsbGD,Remote Desktop Generic USB
Device,\SystemRoot\system32\drivers\TsUsbGD.sys,,Manual,
Fri Feb 20 18:23:16 2015Z,cphs,Intel(R) Content Protection HECI
Service,%SystemRoot%\SysWow64\IntelCpHeciSvc.exe,,Manual,****LocalSystem
Fri Feb 20 18:22:35 2015Z,{FD2B5103-617C-4AE6-8DC4-A4772C463DDC},,,^,^,^,^,,
Fri Feb 20 17:05:34 2015Z,vcsFPSvc,Validity VCS Fingerprint
Service,C:\Windows\system32\vcsFPSvc.exe,,Auto Start,****LocalSystem
Fri Feb 20 16:54:33 2015Z,AtiHDAudioService,AMD Function Driver for HD Audio
Service,system32\drivers\AtihdW76.sys,,Manual,
Fri Feb 20 16:54:27 2015Z,amdcmpag,,system32\DRIVERS\atikmpag.sys,,Manual,
Fri Feb 20 16:54:14 2015Z,{3ED9F155-8201-430C-85E1-EDD7020DE0CF},,,^,^,^,^,,
Fri Feb 20 16:53:55 2015Z,AMD External Events
Utility,,%SystemRoot%\system32\atiesrxx.exe,,Auto Start,****LocalSystem
Fri Feb 20 16:53:55 2015Z,Atierecord,,^,^,^,^,,
Fri Feb 20 16:53:55 2015Z,iphlpvc\Parameters,,%SystemRoot%\System32\iphlpvc.dll,,
Fri Feb 20 16:53:49 2015Z,{8B32CCEF-F092-453D-A04B-084246668014},,,^,^,^,^,,
Fri Feb 20 16:53:43 2015Z,{749B2830-EBF4-4268-8BFD-189D3224ACFB},,,^,^,^,^,,
Fri Feb 20 16:53:35 2015Z,hpsrv,HP Service,%SystemRoot%\system32\Hpsservice.exe,,Auto
Start,****LocalSystem
Fri Feb 20 16:53:06 2015Z,ohci1394,1394 OHCI Compliant Host Controller
(Legacy),\SystemRoot\system32\drivers\ohci1394.sys,,Manual,
Mon Dec 1 14:38:46
2014Z,SysMain,@%SystemRoot%\system32\sysmain.dll;-1000,%systemroot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Mon Dec 1 14:16:45
2014Z,WatAdminSvc,@%SystemRoot%\system32\Wat\WatUX.exe;-601,%SystemRoot%\system32\Wa
t\WatAdminSvc.exe,,Manual,****LocalSystem

```

## SYSTEM OUTPUT

```

Mon Dec 1 14:14:27 2014Z,gpsvc,@gpapi.dll;-112,%windir%\system32\svchost.exe -k
GPSvcGroup,,Auto Start,****LocalSystem
Mon Dec 1 14:13:22
2014Z,IEEtwCollectorService,@%SystemRoot%\system32\ieetwcollectorres.dll;-1000,%SystemRoot%\system32\IEEtwCollector.exe /V,,Manual,****LocalSystem
Mon Dec 1 14:13:22 2014Z,RDPUDP,,,^,,,
Mon Dec 1 14:13:22 2014Z,RdpVideoMiniport,Remote Desktop Video Miniport
Driver,System32\drivers\rdpvideominiport.sys,,Manual,
Mon Dec 1 14:13:22 2014Z,WinHttpAutoProxySvc\Parameters,,winhttp.dll,,,
Mon Dec 1 14:01:16 2014Z,MSDTC Bridge 3.0.0.0,,,^,,,
Mon Dec 1 14:01:16 2014Z,ServiceModelEndpoint 3.0.0.0,,,^,,,
Mon Dec 1 14:01:16 2014Z,ServiceModelOperation 3.0.0.0,,,^,,,
Mon Dec 1 14:01:16 2014Z,ServiceModelService 3.0.0.0,,,^,,,
Mon Dec 1 14:01:16 2014Z,SMsvchost 3.0.0.0,,,^,,,
Mon Dec 1 14:01:16 2014Z,Windows Workflow Foundation 3.0.0.0,,,^,,,
Mon Dec 1 13:04:59
2014Z,wuauerv,@%systemroot%\system32\wuaueng.dll;-105,%systemroot%\system32\svchost
.exe -k netsvcs,,Auto Start,****LocalSystem
Mon Dec 1 13:00:30 2014Z,Wlansvc\Parameters,,%SystemRoot%\System32\wlansvc.dll,,,
Mon Dec 1 12:59:32 2014Z,BTHPORT,Bluetooth Port
Driver,System32\Drivers\BTHport.sys,,Manual,
Mon Dec 1 12:59:19
2014Z,Wlansvc,@%SystemRoot%\System32\wlansvc.dll;-257,%SystemRoot%\system32\svchost.
exe -k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Sat Nov 29 16:11:45
2014Z,WebClient,@%systemroot%\system32\webclnt.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Sat Nov 29 16:10:13 2014Z,ProfSvc\Parameters,,%systemroot%\system32\profsvc.dll,,,
Sat Nov 29 16:10:13 2014Z,WebClient\Parameters,,%SystemRoot%\System32\webclnt.dll,,,
Sat Nov 29 16:07:24
2014Z,wudfsvc,@%SystemRoot%\system32\wudfsvc.dll;-1000,%SystemRoot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Sat Nov 29 16:06:59
2014Z,FontCache,@%systemroot%\system32\FntCache.dll;-100,%SystemRoot%\system32\svcho
st.exe -k LocalService,,Auto Start,****NT AUTHORITY\LocalService
Sat Nov 29 16:06:59
2014Z,FontCache\Parameters,,%SystemRoot%\system32\FntCache.dll,,,
Tue Apr 12 08:29:05
2011Z,CscService,@%systemroot%\system32\cscsvc.dll;-200,%SystemRoot%\System32\svchos
t.exe -k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Tue Apr 12 08:28:48
2011Z,AppMgmt,@appmgmts.dll;-3250,%SystemRoot%\system32\svchost.exe -k
netsvcs,,Manual,****LocalSystem
Tue Apr 12 08:28:48
2011Z,ehRecvr,@%SystemRoot%\ehome\ehrecvr.exe;-101,%systemroot%\ehome\ehRecvr.exe,,M
anual,****NT AUTHORITY\networkService
Tue Apr 12 08:28:48
2011Z,ehSched,@%SystemRoot%\ehome\ehsched.exe;-101,%systemroot%\ehome\ehsched.exe,,M

```



## SYSTEM OUTPUT

```

anual,****NT AUTHORITY\networkService
Tue Apr 12 08:28:48
2011Z,Mcx2Svc,@%SystemRoot%\ehome\ehres.dll;-15501,%SystemRoot%\system32\svchost.exe
-k LocalServiceAndNoImpersonation,,Disabled,****NT Authority\LocalService
Tue Apr 12 08:28:48
2011Z,PeerDistSvc,@%SystemRoot%\system32\peerdistsvc.dll;-9000,%SystemRoot%\System32
\svchost.exe -k PeerDist,,Manual,****NT AUTHORITY\NetworkService
Tue Apr 12 08:28:48 2011Z,RDPDR,Terminal Server Device Redirector
Driver,System32\drivers\rdpdr.sys,,Manual,
Tue Apr 12 08:28:48
2011Z,SensrSvc,@%SystemRoot%\System32\sensrsvc.dll;-1000,%SystemRoot%\system32\svcho
st.exe -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Tue Apr 12 08:28:48
2011Z,StorSvc,@%SystemRoot%\System32\StorSvc.dll;-100,%SystemRoot%\System32\svchost.
exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Tue Apr 12 08:28:48
2011Z,UmRdpService,@%SystemRoot%\system32\umrdp.dll;-1000,%SystemRoot%\System32\svch
ost.exe -k LocalSystemNetworkRestricted,,Manual,****localSystem
Tue Apr 12 08:28:45 2011Z,AppMgmt\Parameters,,%SystemRoot%\System32\appmgmts.dll,,,
Tue Apr 12 08:28:45 2011Z,CscService\Parameters,,%SystemRoot%\System32\cscsvc.dll,,,
Tue Apr 12 08:28:45 2011Z,Mcx2Svc\Parameters,,%SystemRoot%\system32\Mcx2Svc.dll,,,
Tue Apr 12 08:28:45
2011Z,PeerDistSvc\Parameters,,%SystemRoot%\system32\peerdistsvc.dll,,,
Tue Apr 12 08:28:45 2011Z,SensrSvc\Parameters,,%SystemRoot%\system32\sensrsvc.dll,,,
Tue Apr 12 08:28:45 2011Z,StorSvc\Parameters,,%SystemRoot%\system32\storsvc.dll,,,
Tue Apr 12 08:28:45
2011Z,UmRdpService\Parameters,,%SystemRoot%\System32\umrdp.dll,,,
Tue Apr 12 08:27:52 2011Z,dmrvsc,,\SystemRoot\system32\drivers\dmrvsc.sys,,Manual,
Tue Apr 12 08:27:52 2011Z,s3cap,,\SystemRoot\system32\drivers\ms3cap.sys,,Manual,
Tue Apr 12 08:27:52
2011Z,VMBusHID,,\SystemRoot\system32\drivers\VMBusHID.sys,,Manual,
Sun Nov 21 03:58:24 2010Z,BTHMODEM,Bluetooth Serial Communications
Driver,\SystemRoot\system32\drivers\bthmodem.sys,,Manual,
Sun Nov 21 03:58:22 2010Z,gagp30kx,Microsoft Generic AGPv3.0 Filter for K8 Processor
Platforms,\SystemRoot\system32\drivers\gagp30kx.sys,,Manual,
Sun Nov 21 03:58:22 2010Z,uagp35,Microsoft AGPv3.5
Filter,\SystemRoot\system32\drivers\uagp35.sys,,Manual,
Sun Nov 21 03:58:21 2010Z,b06bdrv,Broadcom NetXtreme II
VBD,\SystemRoot\system32\drivers\bxbvda.sys,,Manual,
Sun Nov 21 03:58:21 2010Z,HidBth,Microsoft Bluetooth HID
Miniport,\SystemRoot\system32\drivers\hidbth.sys,,Manual,
Sun Nov 21 03:58:19 2010Z,AmdK8,AMD K8 Processor
Driver,\SystemRoot\system32\drivers\amdK8.sys,,Manual,
Sun Nov 21 03:58:19 2010Z,AmdPPM,AMD Processor
Driver,\SystemRoot\system32\drivers\amdppm.sys,,Manual,
Sun Nov 21 03:58:19 2010Z,Processor,Processor
Driver,\SystemRoot\system32\drivers\processr.sys,,Manual,
Sun Nov 21 03:58:18 2010Z,ebdrv,Broadcom NetXtreme II 10 GigE

```

## SYSTEM OUTPUT

VBD, \SystemRoot\system32\drivers\evbda.sys,,Manual,  
Sun Nov 21 03:58:18 2010Z,fdc,Floppy Disk Controller  
Driver, \SystemRoot\system32\drivers\fdc.sys,,Manual,  
Sun Nov 21 03:58:17 2010Z,pcmcia,,\SystemRoot\system32\drivers\pcmcia.sys,,Manual,  
Sun Nov 21 03:58:16 2010Z,MTConfig,Microsoft Input Configuration  
Driver, \SystemRoot\system32\drivers\MTConfig.sys,,Manual,  
Sun Nov 21 03:58:15 2010Z,circlass,Consumer IR  
Devices, \SystemRoot\system32\drivers\circlass.sys,,Manual,  
Sun Nov 21 03:58:13 2010Z,flpydisk,Floppy Disk  
Driver, \SystemRoot\system32\drivers\flpydisk.sys,,Manual,  
Sun Nov 21 03:58:13 2010Z,sfloppy,High-Capacity Floppy Disk  
Drive, \SystemRoot\system32\drivers\sfloppy.sys,,Manual,  
Sun Nov 21 03:58:11 2010Z,HidBatt,HID UPS Battery  
Driver, \SystemRoot\system32\drivers\HidBatt.sys,,Manual,  
Sun Nov 21 03:58:08 2010Z,HidIr,Microsoft Infrared HID  
Driver, \SystemRoot\system32\drivers\hidir.sys,,Manual,  
Sun Nov 21 03:58:07 2010Z,sermouse,Serial Mouse  
Driver, \SystemRoot\system32\drivers\sermouse.sys,,Manual,  
Sun Nov 21 03:58:06 2010Z,BrFiltLo,Brother USB Mass-Storage Lower Filter  
Driver, \SystemRoot\system32\drivers\BrFiltLo.sys,,Manual,  
Sun Nov 21 03:58:06 2010Z,BrFiltUp,Brother USB Mass-Storage Upper Filter  
Driver, \SystemRoot\system32\drivers\BrFiltUp.sys,,Manual,  
Sun Nov 21 03:58:05 2010Z,usbohci,Microsoft USB Open Host Controller Miniport  
Driver, \SystemRoot\system32\drivers\usbohci.sys,,Manual,  
Sun Nov 21 03:58:05 2010Z,usbuhci,Microsoft USB Universal Host Controller Miniport  
Driver, \SystemRoot\system32\drivers\usbuhci.sys,,Manual,  
Sun Nov 21 03:58:00 2010Z,WacomPen,Wacom Serial Pen HID  
Driver, \SystemRoot\system32\drivers\wacompen.sys,,Manual,  
Sun Nov 21 03:57:59 2010Z,crcdisk,Crcdisk Filter  
Driver, \SystemRoot\system32\drivers\crcdisk.sys,,Disabled,  
Sun Nov 21 03:57:58 2010Z,UmPass,Microsoft UMPass  
Driver, \SystemRoot\system32\drivers\umpass.sys,,Manual,  
Sun Nov 21 03:46:56 2010Z,b57nd60a,Broadcom NetXtreme Gigabit Ethernet - NDIS  
6.0,system32\DRIVERS\b57nd60a.sys,,Manual,  
Sun Nov 21 03:46:56 2010Z,vga,,system32\DRIVERS\vgapnp.sys,,Manual,  
Sun Nov 21 03:39:53 2010Z,Dhcp\Parameters,,%SystemRoot%\system32\dhcpcore.dll,,,  
Sun Nov 21 03:38:46 2010Z,TsUsbFlt,,system32\drivers\tsusbflt.sys,,Manual,  
Sun Nov 21 03:33:56  
2010Z,SessionEnv,@%SystemRoot%\System32\SessEnv.dll;-1026,%SystemRoot%\System32\svch  
ost.exe -k netsvcs,,Manual,\*\*\*localSystem  
Sun Nov 21 03:29:32 2010Z,AcpiPmi,ACPI Power Meter  
Driver, \SystemRoot\system32\drivers\acpipmi.sys,,Manual,  
Sun Nov 21 03:29:32 2010Z,agp440,Intel AGP Bus  
Filter, \SystemRoot\system32\drivers\agp440.sys,,Manual,  
Sun Nov 21 03:29:32 2010Z,amdxata,,system32\drivers\amdxata.sys,,Boot Start,  
Sun Nov 21 03:29:32 2010Z,ErrDev,Microsoft Hardware Error Device  
Driver, \SystemRoot\system32\drivers\errdev.sys,,Manual,  
Sun Nov 21 03:29:32 2010Z,IPMIDrv,,\SystemRoot\system32\drivers\IPMIDrv.sys,,Manual,

## SYSTEM OUTPUT

```

Sun Nov 21 03:29:32 2010Z,iScsiPrt,iScsiPort
Driver,\SystemRoot\system32\drivers\msiscsi.sys,,Manual,
Sun Nov 21 03:29:32 2010Z,nv_agp,NVIDIA nForce AGP Bus
Filter,\SystemRoot\system32\drivers\nv_agp.sys,,Manual,
Sun Nov 21 03:29:32 2010Z,sffdisk,SFF Storage Class
Driver,\SystemRoot\system32\drivers\sffdisk.sys,,Manual,
Sun Nov 21 03:29:32 2010Z,sffp_mmc,SFF Storage Protocol Driver for
MMC,\SystemRoot\system32\drivers\sffp_mmc.sys,,Manual,
Sun Nov 21 03:29:32 2010Z,sffp_sd,SFF Storage Protocol Driver for
SDBus,\SystemRoot\system32\drivers\sffp_sd.sys,,Manual,
Sun Nov 21 03:29:32 2010Z,uliagpkx,Uli AGP Bus
Filter,\SystemRoot\system32\drivers\uliagpkx.sys,,Manual,
Sun Nov 21 03:29:32 2010Z,usbcir,eHome Infrared Receiver
(USBCIR),\SystemRoot\system32\drivers\usbcir.sys,,Manual,
Sun Nov 21 03:29:32 2010Z,vhdmpp,,\SystemRoot\system32\drivers\vhdmpp.sys,,Manual,
Tue Jul 14 05:34:12 2009Z,BDESVC\Parameters,,%SystemRoot%\System32\bdesvc.dll,,,
Tue Jul 14 05:34:12
2009Z,PNRPAutoReg\Parameters,,%SystemRoot%\system32\pnrpauto.dll,,,
Tue Jul 14 05:34:12 2009Z,WPCSvc\Parameters,,%SystemRoot%\System32\wpcsvc.dll,,,
Tue Jul 14 05:34:09 2009Z,p2pimsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,
Tue Jul 14 05:34:09 2009Z,p2psvc\Parameters,,%SystemRoot%\system32\p2psvc.dll,,,
Tue Jul 14 05:34:09 2009Z,SDRSVC\Parameters,,%Systemroot%\System32\SDRSVC.dll,,,
Tue Jul 14 04:54:38 2009Z,NdisCap,NDIS Capture LightWeight
Filter,system32\DRIVERS\ndiscap.sys,,Manual,
Tue Jul 14 04:54:32 2009Z,hkmsvc\Parameters,,%SystemRoot%\system32\kmsvc.dll,,,
Tue Jul 14 04:54:31 2009Z,napagent\Parameters,,%SystemRoot%\system32\qagentRT.dll,,,
Tue Jul 14 04:54:25
2009Z,defragsvc\Parameters,,%Systemroot%\System32\defragsvc.dll,,,
Tue Jul 14 04:54:05 2009Z,WerSvc\Parameters,,%SystemRoot%\System32\WerSvc.dll,,,
Tue Jul 14 04:53:57
2009Z,Smb,@%SystemRoot%\system32\tcpipcfg.dll;-50005,system32\DRIVERS\smb.sys,,Manua
l,
Tue Jul 14 04:53:56 2009Z,lmhosts\Parameters,,%SystemRoot%\System32\lmhsvc.dll,,,
Tue Jul 14 04:53:48 2009Z,THREADORDER\Parameters,,%SystemRoot%\system32\mmcss.dll,,,
Tue Jul 14 04:53:45
2009Z,TrkWks,@%SystemRoot%\system32\trkwks.dll;-1,%SystemRoot%\System32\svchost.exe
-k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Tue Jul 14 04:53:45 2009Z,TrkWks\Parameters,,%SystemRoot%\System32\trkwks.dll,,,
Tue Jul 14 04:53:36
2009Z,RpcEptMapper,@%windir%\system32\RpcEpMap.dll;-1001,%SystemRoot%\system32\svcho
st.exe -k RPCSS,,Auto Start,****NT AUTHORITY\NetworkService
Tue Jul 14 04:53:36
2009Z,RpcEptMapper\Parameters,,%SystemRoot%\System32\RpcEpMap.dll,,,
Tue Jul 14 04:53:33
2009Z,LanmanServer,@%systemroot%\system32\srvsvc.dll;-100,%SystemRoot%\system32\svch
ost.exe -k netsvcs,,Auto Start,****LocalSystem
Tue Jul 14 04:53:31
2009Z,LanmanWorkstation,@%systemroot%\system32\wkssvc.dll;-100,%SystemRoot%\System32

```

## SYSTEM OUTPUT

```

\svchost.exe -k NetworkService,,Auto Start,****NT AUTHORITY\NetworkService
Tue Jul 14 04:53:31
2009Z,LanmanWorkstation\Parameters,,%SystemRoot%\System32\wkssvc.dll,,,
Tue Jul 14 04:53:25 2009Z,WmiApRpl,,,^^^^,,
Tue Jul 14 04:53:24
2009Z,Winmgmt,@%Systemroot%\system32\wbem\wmisvc.dll;-205,%systemroot%\system32\svch
ost.exe -k netsvcs,,Auto Start,****localSystem
Tue Jul 14 04:53:24
2009Z,wmiApSrv,@%Systemroot%\system32\wbem\wmiapsrv.exe;-110,%systemroot%\system32\w
bem\WmiApSrv.exe,,Manual,****localSystem
Tue Jul 14 04:53:21 2009Z,TCPIP6,Microsoft IPv6 Protocol
Driver,system32\DRIVERS\tcpip.sys,,Manual,
Tue Jul 14 04:53:21
2009Z,WANARP,@%systemroot%\system32\rascfg.dll;-32011,system32\DRIVERS\wanarp.sys,,M
anual,
Tue Jul 14 04:53:20
2009Z,lmhosts,@%SystemRoot%\system32\lmhsvc.dll;-101,%SystemRoot%\system32\svchost.e
xe -k LocalServiceNetworkRestricted,,Auto Start,****NT AUTHORITY\LocalService
Tue Jul 14 04:53:19
2009Z,Dhcp,@%SystemRoot%\system32\dhcpcore.dll;-100,%SystemRoot%\system32\svchost.ex
e -k LocalServiceNetworkRestricted,,Auto Start,****NT Authority\LocalService
Tue Jul 14 04:53:19 2009Z,Winsock,,,^^^^4,3,
Tue Jul 14 04:49:48
2009Z,SamSs,@%SystemRoot%\system32\samsrv.dll;-1,%SystemRoot%\system32\lsass.exe,,Au
to Start,****LocalSystem
Tue Jul 14 04:49:48
2009Z,W32Time,@%SystemRoot%\system32\w32time.dll;-200,%SystemRoot%\system32\svchost.
exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:48 2009Z,W32Time\Parameters,,%systemroot%\system32\w32time.dll,,,
Tue Jul 14 04:49:46
2009Z,Dnscache,@%SystemRoot%\System32\dnsapi.dll;-101,%SystemRoot%\system32\svchost.
exe -k NetworkService,,Auto Start,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:46 2009Z,Dnscache\Parameters,,%SystemRoot%\System32\dnsrslvr.dll,,,
Tue Jul 14 04:49:45
2009Z,RemoteAccess,@%Systemroot%\system32\mprdim.dll;-200,%SystemRoot%\System32\svch
ost.exe -k netsvcs,,Disabled,****localSystem
Tue Jul 14 04:49:45
2009Z,RemoteAccess\Parameters,,%SystemRoot%\System32\mprdim.dll,,,
Tue Jul 14 04:49:35
2009Z,RasAuto,@%Systemroot%\system32\rasauto.dll;-200,%SystemRoot%\System32\svchost.
exe -k netsvcs,,Manual,****localSystem
Tue Jul 14 04:49:35 2009Z,RasAuto\Parameters,,%SystemRoot%\System32\rasauto.dll,,,
Tue Jul 14 04:49:35
2009Z,RasMan,@%Systemroot%\system32\rasmans.dll;-200,%SystemRoot%\System32\svchost.e
xe -k netsvcs,,Manual,****localSystem
Tue Jul 14 04:49:35 2009Z,RasMan\Parameters,,%SystemRoot%\System32\rasmans.dll,,,
Tue Jul 14 04:49:26 2009Z,SstpSvc\Parameters,,%SystemRoot%\system32\sstpsvc.dll,,,
Tue Jul 14 04:49:24

```

## SYSTEM OUTPUT

```

2009Z,DPS,@%systemroot%\system32\dps.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,,Auto Start,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:24 2009Z,DPS\Parameters,,%SystemRoot%\system32\dps.dll,,,
Tue Jul 14 04:49:24
2009Z,WdiServiceHost,@%systemroot%\system32\wdi.dll;-502,%SystemRoot%\System32\svcho
st.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:24
2009Z,WdiServiceHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Tue Jul 14 04:49:24
2009Z,WdiSystemHost,@%systemroot%\system32\wdi.dll;-500,%SystemRoot%\System32\svchos
t.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Tue Jul 14 04:49:24 2009Z,WdiSystemHost\Parameters,,%SystemRoot%\system32\wdi.dll,,,
Tue Jul 14 04:49:23 2009Z,EapHost\Parameters,,%SystemRoot%\System32\eapsvc.dll,,,
Tue Jul 14 04:49:20 2009Z,gpsvc\Parameters,,%SystemRoot%\System32\gpsvc.dll,,,
Tue Jul 14 04:49:20 2009Z,NlaSvc\Parameters,,%SystemRoot%\System32\nlasvc.dll,,,
Tue Jul 14 04:49:18 2009Z,BITS\Parameters,,%SystemRoot%\System32\qmgr.dll,,,
Tue Jul 14 04:49:08 2009Z,nsi\Parameters,,%systemroot%\system32\nsisvc.dll,,,
Tue Jul 14 04:49:01 2009Z,.NET CLR Data,,,^^^,,
Tue Jul 14 04:49:01 2009Z,.NET CLR Networking,,,^^^,,
Tue Jul 14 04:49:01 2009Z,.NET Data Provider for Oracle,,,^^^,,
Tue Jul 14 04:49:01 2009Z,.NET Data Provider for SqlServer,,,^^^,,
Tue Jul 14 04:49:01 2009Z,.NETFramework,,,^^^,,
Tue Jul 14 04:49:01 2009Z,adsi,,,^^^,,
Tue Jul 14 04:49:01
2009Z,AeLookupSvc,@%SystemRoot%\system32\aelupsvc.dll;-1,%systemroot%\system32\svcho
st.exe -k netsvcs,,Manual,****localSystem
Tue Jul 14 04:49:01
2009Z,AeLookupSvc\Parameters,,%SystemRoot%\System32\aelupsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,ALG,@%SystemRoot%\system32\Alg.exe;-112,%SystemRoot%\System32\alg.exe,,Manual,
****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,AppID,@%systemroot%\system32\appidsvc.dll;-102,\SystemRoot\system32\drivers\ap
pid.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,AppIDSvc,@%systemroot%\system32\appidsvc.dll;-100,%SystemRoot%\system32\svchos
t.exe -k LocalServiceAndNoImpersonation,,Manual,****NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,AppIDSvc\Parameters,,%SystemRoot%\System32\appidsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,Appinfo,@%systemroot%\system32\appinfo.dll;-100,%SystemRoot%\system32\svchost.
exe -k netsvcs,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,Appinfo\Parameters,,%SystemRoot%\System32\appinfo.dll,,,
Tue Jul 14 04:49:01
2009Z,AudioEndpointBuilder,@%SystemRoot%\system32\audiosrv.dll;-204,%SystemRoot%\Sys
tem32\svchost.exe -k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01
2009Z,AudioEndpointBuilder\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,
Tue Jul 14 04:49:01

```

## SYSTEM OUTPUT

```

2009Z,AudioSrv,@%SystemRoot%\system32\audiosrv.dll;-200,%SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted,,Auto Start,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,AudioSrv\Parameters,,%SystemRoot%\System32\Audiosrv.dll,,,
Tue Jul 14 04:49:01
2009Z,AxInstSV,@%SystemRoot%\system32\AxInstSV.dll;-103,%SystemRoot%\system32\svchost.exe -k AxInstSVGroup,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,AxInstSV\Parameters,,%SystemRoot%\System32\AxInstSV.dll,,,
Tue Jul 14 04:49:01 2009Z,BattC,,,^ ^ ^ ^,,
Tue Jul 14 04:49:01
2009Z,BDESVC,@%SystemRoot%\system32\bdesvc.dll;-100,%SystemRoot%\System32\svchost.exe -k netsvcs,,Manual,****localSystem
Tue Jul 14 04:49:01
2009Z,BFE,@%SystemRoot%\system32\bfe.dll;-1001,%systemroot%\system32\svchost.exe -k LocalServiceNoNetwork,,Auto Start,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,BFE\Parameters,,%SystemRoot%\System32\bfe.dll,,,
Tue Jul 14 04:49:01
2009Z,Browser,@%systemroot%\system32\browser.dll;-100,%SystemRoot%\System32\svchost.exe -k netsvcs,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,Browser\Parameters,,%SystemRoot%\System32\browser.dll,,,
Tue Jul 14 04:49:01 2009Z,Brserid,Brother MFC Serial Port Interface Driver (WDM),\SystemRoot\System32\Drivers\Brserid.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,BrSerWdm,Brother WDM Serial driver,\SystemRoot\System32\Drivers\BrSerWdm.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,BrUsbMdm,Brother MFC USB Fax Only Modem,\SystemRoot\System32\Drivers\BrUsbMdm.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,BrUsbSer,Brother MFC USB Serial WDM Driver,\SystemRoot\System32\Drivers\BrUsbSer.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,bthserv,@%SystemRoot%\System32\bthserv.dll;-101,%SystemRoot%\system32\svchost.exe -k bthsvcs,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,bthserv\Parameters,,%SystemRoot%\system32\bthserv.dll,,,
Tue Jul 14 04:49:01
2009Z,CertPropSvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,
Tue Jul 14 04:49:01
2009Z,COMSysApp,@comres.dll;-947,%SystemRoot%\system32\dlhhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235},,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,crypt32,,,^ ^ ^ ^,,
Tue Jul 14 04:49:01
2009Z,CryptSvc,@%SystemRoot%\system32\cryptsvc.dll;-1001,%SystemRoot%\system32\svchost.exe -k NetworkService,,Auto Start,****NT Authority\NetworkService
Tue Jul 14 04:49:01 2009Z,CryptSvc\Parameters,,%SystemRoot%\system32\cryptsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,DCLocator,,,^ ^ ^ ^,,
Tue Jul 14 04:49:01
2009Z,DcomLaunch,@oleres.dll;-5012,%SystemRoot%\system32\svchost.exe -k DcomLaunch,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01
2009Z,defragsvc,@%SystemRoot%\system32\defragsvc.dll;-101,%SystemRoot%\system32\svchost.exe -k defragsvc,,Manual,****localSystem

```

## SYSTEM OUTPUT

```

Tue Jul 14 04:49:01
2009Z,dot3svc,@%systemroot%\system32\dot3svc.dll;-1102,%SystemRoot%\system32\svchost
.exe -k LocalSystemNetworkRestricted,,Manual,****localSystem
Tue Jul 14 04:49:01 2009Z,dot3svc\Parameters,,%SystemRoot%\System32\dot3svc.dll,,,
Tue Jul 14 04:49:01
2009Z,EFS,@%SystemRoot%\system32\efssvc.dll;-100,%SystemRoot%\System32\lsass.exe,,Ma
nual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,ESENT,,,^^^,,
Tue Jul 14 04:49:01
2009Z,EventSystem,@comres.dll;-2450,%SystemRoot%\system32\svchost.exe -k
LocalService,,Auto Start,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,EventSystem\Parameters,,%systemroot%\system32\es.dll,,,
Tue Jul 14 04:49:01
2009Z,Fax,@%systemroot%\system32\fxsresm.dll;-118,%systemroot%\system32\fxssvc.exe,,
Manual,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,fdPHost,@%systemroot%\system32\fdPHost.dll;-100,%SystemRoot%\system32\svchost.
exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,fdPHost\Parameters,,%SystemRoot%\system32\fdPHost.dll,,,
Tue Jul 14 04:49:01 2009Z,FDResPub\Parameters,,%SystemRoot%\system32\fdrespub.dll,,,
Tue Jul 14 04:49:01
2009Z,Filetrace,@%SystemRoot%\system32\drivers\filetrace.sys;-10001,system32\drivers
\filetrace.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,FontCache3.0.0.0,@%SystemRoot%\system32\PresentationHost.exe;-3309,%systemroot
%\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe,,Manual,****NT
Authority\LocalService
Tue Jul 14 04:49:01
2009Z,FsDepends,@%SystemRoot%\system32\drivers\fsdepends.sys;-10001,system32\drivers
\FsDepends.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,hcw85cir,Hauppage Consumer Infrared
Receiver,\SystemRoot\system32\drivers\hwc85cir.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,hidserv,@%SystemRoot%\System32\hidserv.dll;-101,%SystemRoot%\system32\svchost.
exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,hidserv\Parameters,,%SystemRoot%\system32\hidserv.dll,,,
Tue Jul 14 04:49:01
2009Z,hkmsvc,@%SystemRoot%\system32\kmsvc.dll;-6,%SystemRoot%\System32\svchost.exe
-k netsvcs,,Manual,****localSystem
Tue Jul 14 04:49:01
2009Z,HomeGroupListener\Parameters,,%SystemRoot%\system32>ListSvc.dll,,,
Tue Jul 14 04:49:01
2009Z,HomeGroupProvider,@%SystemRoot%\System32\provsvc.dll;-100,%SystemRoot%\System3
2\svchost.exe -k LocalServiceNetworkRestricted,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,HomeGroupProvider\Parameters,,%SystemRoot%\system32\provsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,idsvc,@%systemroot%\Microsoft.NET\Framework64\v3.0\Windows
Communication

```

## SYSTEM OUTPUT

```

Foundation\ServiceModelInstallRC.dll;-8193,"%systemroot%\Microsoft.NET\Framework64\v
3.0\Windows Communication Foundation\infocard.exe",,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,IKEEXT\Parameters,,%SystemRoot%\System32\ikeext.dll,,
Tue Jul 14 04:49:01 2009Z,inetaccs,,,^ ^ ^ ^,,
Tue Jul 14 04:49:01
2009Z,IPBusEnum,@%systemroot%\system32\IPBusEnum.dll;-102,%SystemRoot%\system32\svch
ost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Tue Jul 14 04:49:01
2009Z,IPBusEnum\Parameters,,%SystemRoot%\system32\ipbusenum.dll,,
Tue Jul 14 04:49:01
2009Z,IpFilterDriver,@%systemroot%\system32\rascfg.dll;-32013,system32\DRIVERS\ipflt
drv.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,iphlpvc,@%SystemRoot%\system32\iphlpvc.dll;-500,%SystemRoot%\System32\svchos
t.exe -k NetSvc,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01 2009Z,IPNAT,IP Network Address
Translator,System32\drivers\ipnat.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,IRENUM,@%SystemRoot%\system32\drivers\irenum.sys;-100,system32\drivers\irenum.
sys,,Manual,
Tue Jul 14 04:49:01
2009Z,KeyIso,@keyiso.dll;-100,%SystemRoot%\system32\lsass.exe,,Manual,****LocalSyste
m
Tue Jul 14 04:49:01 2009Z,KtmRm,@comres.dll;-2946,%SystemRoot%\System32\svchost.exe
-k NetworkServiceAndNoImpersonation,,Manual,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,KtmRm\Parameters,,%systemroot%\system32\msdtckrm.dll,,
Tue Jul 14 04:49:01 2009Z,ldap,,,^ ^ ^ ^,,
Tue Jul 14 04:49:01
2009Z,lltdsvc,@%SystemRoot%\system32\lltdres.dll;-1,%SystemRoot%\System32\svchost.ex
e -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,lltdsvc\Parameters,,%SystemRoot%\System32\lltdsvc.dll,,
Tue Jul 14 04:49:01 2009Z,Lsa,,,^ ^ ^ ^,,
Tue Jul 14 04:49:01
2009Z,MMCSS,@%systemroot%\system32\mmcscs.dll;-100,%SystemRoot%\system32\svchost.exe
-k netsvc,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01 2009Z,MMCSS\Parameters,,%SystemRoot%\system32\mmcscs.dll,,
Tue Jul 14 04:49:01
2009Z,MpsSvc,@%SystemRoot%\system32\FirewallAPI.dll;-23090,%SystemRoot%\system32\svc
host.exe -k LocalServiceNoNetwork,,Auto Start,****NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,MpsSvc\Parameters,,%SystemRoot%\system32\mpssvc.dll,,
Tue Jul 14 04:49:01
2009Z,MRxDAV,@%systemroot%\system32\webclnt.dll;-104,\SystemRoot\system32\drivers\mr
xdav.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,MSDTC,@comres.dll;-2797,%SystemRoot%\System32\msdtc.exe,,Manual,****NT
AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,mshidkmdf,@%SystemRoot%\system32\drivers\mshidkmdf.sys;-100,\SystemRoot\System

```



## SYSTEM OUTPUT

```

32\drivers\mshidkmdf.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,MSiSCSI,@%SystemRoot%\system32\iscsidsc.dll;-5000,%systemroot%\system32\svchos
t.exe -k netsvcs,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,MSiSCSI\Parameters,,%systemroot%\system32\iscsiexe.dll,,
Tue Jul 14 04:49:01 2009Z,MsRPC,,,,Manual,
Tue Jul 14 04:49:01 2009Z,MSSCNTRS,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,napagent,@%SystemRoot%\system32\qagentrt.dll;-6,%SystemRoot%\System32\svchost.
exe -k NetworkService,,Manual,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,Netlogon,@%SystemRoot%\System32\netlogon.dll;-102,%systemroot%\system32\lsass.
exe,,Manual,****LocalSystem
Tue Jul 14 04:49:01
2009Z,Netman,@%SystemRoot%\system32\netman.dll;-109,%SystemRoot%\System32\svchost.ex
e -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,Netman\Parameters,,%SystemRoot%\System32\netman.dll,,
Tue Jul 14 04:49:01
2009Z,netprofm,@%SystemRoot%\system32\netprofm.dll;-202,%SystemRoot%\System32\svchos
t.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,netprofm\Parameters,,%SystemRoot%\System32\netprofm.dll,,
Tue Jul 14 04:49:01
2009Z,NlaSvc,@%SystemRoot%\System32\nlasvc.dll;-1,%SystemRoot%\System32\svchost.exe
-k NetworkService,,Auto Start,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,nsi,@%SystemRoot%\system32\nsisvc.dll;-200,%systemroot%\system32\svchost.exe
-k LocalService,,Auto Start,****NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,NTDS,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,p2pimsvc,@%SystemRoot%\system32\pnprpsvc.dll;-8004,%SystemRoot%\System32\svchos
t.exe -k LocalServicePeerNet,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,p2psvc,@%SystemRoot%\system32\p2psvc.dll;-8006,%SystemRoot%\System32\svchost.e
xe -k LocalServicePeerNet,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,PcaSvc,@%SystemRoot%\system32\pcasvc.dll;-1,%systemroot%\system32\svchost.exe
-k LocalSystemNetworkRestricted,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01 2009Z,PcaSvc\Parameters,,%SystemRoot%\System32\pcasvc.dll,,
Tue Jul 14 04:49:01 2009Z,PerfDisk,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,PerfHost,@%systemroot%\sysWow64\perfhost.exe;-2,%SystemRoot%\SysWow64\perfhost
.exe,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,PerfNet,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,PerfOS,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,PerfProc,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,pla,@%systemroot%\system32\pla.dll;-500,%SystemRoot%\System32\svchost.exe -k
LocalServiceNoNetwork,,Manual,****NT AUTHORITY\LocalService

```

## SYSTEM OUTPUT

Tue Jul 14 04:49:01 2009Z,pla\Parameters,,%systemroot%\system32\pla.dll,,,  
 Tue Jul 14 04:49:01  
 2009Z,PlugPlay,@%SystemRoot%\system32\umpnpmgr.dll;-100,%SystemRoot%\system32\svchost.exe -k DcomLaunch,,Auto Start,\*\*\*\*LocalSystem  
 Tue Jul 14 04:49:01  
 2009Z,PNRPAutoReg,@%SystemRoot%\system32\pnrpauto.dll;-8002,%SystemRoot%\System32\svchost.exe -k LocalServicePeerNet,,Manual,\*\*\*\*NT AUTHORITY\LocalService  
 Tue Jul 14 04:49:01  
 2009Z,PNRPsvc,@%SystemRoot%\system32\pnrpsvc.dll;-8000,%SystemRoot%\System32\svchost.exe -k LocalServicePeerNet,,Manual,\*\*\*\*NT AUTHORITY\LocalService  
 Tue Jul 14 04:49:01 2009Z,PNRPsvc\Parameters,,%SystemRoot%\system32\pnrpsvc.dll,,,  
 Tue Jul 14 04:49:01  
 2009Z,PolicyAgent,@%SystemRoot%\System32\polstore.dll;-5010,%SystemRoot%\system32\svchost.exe -k NetworkServiceNetworkRestricted,,Manual,\*\*\*\*NT Authority\NetworkService  
 Tue Jul 14 04:49:01  
 2009Z,PolicyAgent\Parameters,,%SystemRoot%\System32\ipsecsvc.dll,,,  
 Tue Jul 14 04:49:01 2009Z,PortProxy,,,^^^^,,  
 Tue Jul 14 04:49:01  
 2009Z,Power,@%SystemRoot%\system32\umpo.dll;-100,%SystemRoot%\system32\svchost.exe -k DcomLaunch,,Auto Start,\*\*\*\*LocalSystem  
 Tue Jul 14 04:49:01 2009Z,Power\Parameters,,%SystemRoot%\system32\umpo.dll,,,  
 Tue Jul 14 04:49:01  
 2009Z,ProfSvc,@%systemroot%\system32\profsvc.dll;-300,%systemroot%\system32\svchost.exe -k netsvcs,,Auto Start,\*\*\*\*LocalSystem  
 Tue Jul 14 04:49:01  
 2009Z,ProtectedStorage,@%systemroot%\system32\psbase.dll;-300,%SystemRoot%\system32\lsass.exe,,Manual,\*\*\*\*LocalSystem  
 Tue Jul 14 04:49:01  
 2009Z,QWAVE,@%SystemRoot%\system32\qwave.dll;-1,%windir%\system32\svchost.exe -k LocalServiceAndNoImpersonation,,Manual,\*\*\*\*NT AUTHORITY\LocalService  
 Tue Jul 14 04:49:01 2009Z,QWAVE\Parameters,,%windir%\system32\qwave.dll,,,  
 Tue Jul 14 04:49:01  
 2009Z,QWAVEdrv,@%SystemRoot%\system32\drivers\qwavedrv.sys;-1,\SystemRoot\system32\drivers\qwavedrv.sys,,Manual,  
 Tue Jul 14 04:49:01 2009Z,RasAcd,Remote Access Auto Connection Driver,System32\DRIVERS\rasacd.sys,,Manual,  
 Tue Jul 14 04:49:01 2009Z,RDPDD,,,^^^^,,  
 Tue Jul 14 04:49:01 2009Z,RDPNP,@%systemroot%\system32\drprov.dll;-100,,,^^^^,,  
 Tue Jul 14 04:49:01 2009Z,RDPWD,RDP Winstation Driver,,,Manual,  
 Tue Jul 14 04:49:01  
 2009Z,RemoteRegistry,@regsvc.dll;-1,%SystemRoot%\system32\svchost.exe -k regsvc,,Manual,\*\*\*\*NT AUTHORITY\LocalService  
 Tue Jul 14 04:49:01  
 2009Z,RemoteRegistry\Parameters,,%SystemRoot%\system32\regsvc.dll,,,  
 Tue Jul 14 04:49:01  
 2009Z,RpcLocator,@%systemroot%\system32\Locator.exe;-2,%SystemRoot%\system32\locator.exe,,Manual,\*\*\*\*NT AUTHORITY\NetworkService  
 Tue Jul 14 04:49:01 2009Z,RpcSs,@oleres.dll;-5010,%SystemRoot%\system32\svchost.exe

## SYSTEM OUTPUT

```

-k rpcss,,Auto Start,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,SCardSvr\Parameters,,%SystemRoot%\System32\SCardSvr.dll,,,
Tue Jul 14 04:49:01
2009Z,Schedule,@%SystemRoot%\system32\schedsvc.dll;-100,%systemroot%\system32\svchos
t.exe -k netsvcs,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01 2009Z,Schedule\Parameters,,%systemroot%\system32\schedsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,SCPolicySvc,@%SystemRoot%\System32\certprop.dll;-13,%SystemRoot%\system32\svch
ost.exe -k netsvcs,,Manual,****LocalSystem
Tue Jul 14 04:49:01
2009Z,SCPolicySvc\Parameters,,%SystemRoot%\System32\certprop.dll,,,
Tue Jul 14 04:49:01
2009Z,SDRSVC,@%SystemRoot%\system32\sdrsvc.dll;-107,%SystemRoot%\system32\svchost.ex
e -k SDRSVC,,Manual,****localSystem
Tue Jul 14 04:49:01
2009Z,seclogon,@%SystemRoot%\system32\seclogon.dll;-7001,%windir%\system32\svchost.e
xe -k netsvcs,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,seclogon\Parameters,,%windir%\system32\seclogon.dll,,,
Tue Jul 14 04:49:01
2009Z,SENS,@%SystemRoot%\system32\Sens.dll;-200,%SystemRoot%\system32\svchost.exe -k
netsvcs,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01 2009Z,SENS\Parameters,,%SystemRoot%\System32\sens.dll,,,
Tue Jul 14 04:49:01
2009Z,SessionEnv\Parameters,,%SystemRoot%\system32\sessenv.dll,,,
Tue Jul 14 04:49:01
2009Z,ShellHWDetection,@%SystemRoot%\System32\shsvcs.dll;-12288,%SystemRoot%\System3
2\svchost.exe -k netsvcs,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01
2009Z,ShellHWDetection\Parameters,,%SystemRoot%\System32\shsvcs.dll,,,
Tue Jul 14 04:49:01
2009Z,SNMPTRAP,@%SystemRoot%\system32\snmptrap.exe;-3,%SystemRoot%\System32\snmptrap
.exe,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,Spooler,@%systemroot%\system32\spoolsv.exe;-1,%SystemRoot%\System32\spoolsv.ex
e,^^^272,2,LocalSystem
Tue Jul 14 04:49:01
2009Z,sppsvc,@%SystemRoot%\system32\sppsvc.exe;-101,%SystemRoot%\system32\sppsvc.exe
,,Auto Start,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01
2009Z,sppuinotify,@%SystemRoot%\system32\sppuinotify.dll;-103,%SystemRoot%\system32\
svchost.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,sppuinotify\Parameters,,%SystemRoot%\system32\sppuinotify.dll,,,
Tue Jul 14 04:49:01
2009Z,SSDPSRV,@%systemroot%\system32\ssdpsrv.dll;-100,%SystemRoot%\system32\svchost.
exe -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,SSDPSRV\Parameters,,%SystemRoot%\System32\ssdpsrv.dll,,,
Tue Jul 14 04:49:01

```

## SYSTEM OUTPUT

```

2009Z,SstpSvc,@%SystemRoot%\system32\sstpsvc.dll;-200,%SystemRoot%\system32\svchost.
exe -k LocalService,,Manual,****NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,stisvc\Parameters,,%SystemRoot%\System32\wiaservc.dll,,,
Tue Jul 14 04:49:01
2009Z,swprv,@%SystemRoot%\System32\swprv.dll;-103,%SystemRoot%\System32\svchost.exe
-k swprv,,Manual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,swprv\Parameters,,%Systemroot%\System32\swprv.dll,,,
Tue Jul 14 04:49:01 2009Z,SysMain\Parameters,,%systemroot%\system32\sysmain.dll,,,
Tue Jul 14 04:49:01
2009Z,TabletInputService,@%SystemRoot%\system32\TabSvc.dll;-100,%SystemRoot%\System3
2\svchost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Tue Jul 14 04:49:01
2009Z,TabletInputService\Parameters,,%SystemRoot%\System32\TabSvc.dll,,,
Tue Jul 14 04:49:01
2009Z,TapiSrv,@%SystemRoot%\system32\tapisrv.dll;-10100,%SystemRoot%\System32\svchos
t.exe -k NetworkService,,Manual,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,TapiSrv\Parameters,,%SystemRoot%\System32\tapisrv.dll,,,
Tue Jul 14 04:49:01 2009Z,TCPIP6TUNNEL,,,^^^,,
Tue Jul 14 04:49:01 2009Z,TCPIPTUNNEL,,,^^^,,
Tue Jul 14 04:49:01 2009Z,TDPIPE,TDPIPE,system32\drivers\tdpipe.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,TDTCP,TDTCP,system32\drivers\tdtcp.sys,,Manual,
Tue Jul 14 04:49:01
2009Z,TermService,@%SystemRoot%\System32\termsrv.dll;-268,%SystemRoot%\System32\svch
ost.exe -k NetworkService,,Manual,****NT Authority\NetworkService
Tue Jul 14 04:49:01
2009Z,TermService\Parameters,,%SystemRoot%\System32\termsrv.dll,,,
Tue Jul 14 04:49:01
2009Z,Themes,@%SystemRoot%\System32\themeservice.dll;-8192,%SystemRoot%\System32\svc
host.exe -k netsvcs,,Auto Start,****LocalSystem
Tue Jul 14 04:49:01
2009Z,Themes\Parameters,,%SystemRoot%\system32\themeservice.dll,,,
Tue Jul 14 04:49:01
2009Z,THREADORDER,@%systemroot%\system32\mmcsh.dll;-102,%SystemRoot%\system32\svchos
t.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,TSDDD,,,^^^,,
Tue Jul 14 04:49:01
2009Z,tssecsrv,@%SystemRoot%\System32\DRIVERS\tssecsrv.sys;-101,system32\DRIVERS\tss
ecsrv.sys,,Manual,
Tue Jul 14 04:49:01 2009Z,UGatherer,,,^^^,,
Tue Jul 14 04:49:01 2009Z,UGTHRSVC,,,^^^,,
Tue Jul 14 04:49:01
2009Z,UI0Detect,@%SystemRoot%\system32\ui0detect.exe;-101,%SystemRoot%\system32\UI0D
etect.exe,^^^272,3,LocalSystem
Tue Jul 14 04:49:01
2009Z,upnphost,@%systemroot%\system32\upnphost.dll;-213,%SystemRoot%\system32\svchos
t.exe -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,upnphost\Parameters,,%SystemRoot%\System32\upnphost.dll,,,
Tue Jul 14 04:49:01

```

## SYSTEM OUTPUT

```

2009Z,UxSms,@%SystemRoot%\system32\dwm.exe;-2000,%SystemRoot%\System32\svchost.exe
-k LocalSystemNetworkRestricted,,Auto Start,****localSystem
Tue Jul 14 04:49:01 2009Z,UxSms\Parameters,,%SystemRoot%\System32\uxsms.dll,,,
Tue Jul 14 04:49:01
2009Z,VaultSvc,@%SystemRoot%\system32\vaultsvc.dll;-1003,%SystemRoot%\system32\lsass
.exe,,Manual,****LocalSystem
Tue Jul 14 04:49:01
2009Z,vds,@%SystemRoot%\system32\vds.exe;-100,%SystemRoot%\System32\vds.exe,,Manual,
****LocalSystem
Tue Jul 14 04:49:01
2009Z,VSS,@%systemroot%\system32\vssvc.exe;-102,%systemroot%\system32\vssvc.exe,,Man
ual,****LocalSystem
Tue Jul 14 04:49:01 2009Z,W3SVC,,,^^^^,,
Tue Jul 14 04:49:01
2009Z,wbengine,@%systemroot%\system32\wbengine.exe;-104,"%systemroot%\system32\wbeng
ine.exe",,Manual,****localSystem
Tue Jul 14 04:49:01 2009Z,WbioSrvC\Parameters,,%SystemRoot%\System32\wbiosrvC.dll,,,
Tue Jul 14 04:49:01
2009Z,wcncsvc,@%SystemRoot%\system32\wcncsvc.dll;-3,%SystemRoot%\System32\svchost.ex
e -k LocalServiceAndNoImpersonation,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,wcncsvc\Parameters,,%SystemRoot%\System32\wcncsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,WcsPlugInService,@%SystemRoot%\system32\WcsPlugInService.dll;-200,%SystemRoot%
\system32\svchost.exe -k wcscsvc,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,WcsPlugInService\Parameters,,%SystemRoot%\System32\WcsPlugInService.dll,,,
Tue Jul 14 04:49:01
2009Z,Wecsvc,@%SystemRoot%\system32\wecsvc.dll;-200,%SystemRoot%\system32\svchost.ex
e -k NetworkService,,Manual,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,Wecsvc\Parameters,,%SystemRoot%\system32\wecsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,wercplsupport,@%SystemRoot%\System32\wercplsupport.dll;-101,%SystemRoot%\Syste
m32\svchost.exe -k netsvcs,,Manual,****localSystem
Tue Jul 14 04:49:01
2009Z,wercplsupport\Parameters,,%SystemRoot%\System32\wercplsupport.dll,,,
Tue Jul 14 04:49:01
2009Z,WerSvc,@%SystemRoot%\System32\wersvc.dll;-100,%SystemRoot%\System32\svchost.ex
e -k WerSvcGroup,,Manual,****localSystem
Tue Jul 14 04:49:01 2009Z,WinDefend\Parameters,,%ProgramFiles%\Windows
Defender\mpsvc.dll,,,
Tue Jul 14 04:49:01
2009Z,WinHttpAutoProxySvc,@%SystemRoot%\system32\winhttp.dll;-100,%SystemRoot%\syste
m32\svchost.exe -k LocalService,,Manual,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01
2009Z,WinRM,@%Systemroot%\system32\wsmsvc.dll;-101,%SystemRoot%\System32\svchost.exe
-k NetworkService,,Manual,****NT AUTHORITY\NetworkService
Tue Jul 14 04:49:01 2009Z,WinRM\Parameters,,%SystemRoot%\system32\WsmSvc.dll,,,
Tue Jul 14 04:49:01 2009Z,WinSock2,,,^^^^,,

```

## SYSTEM OUTPUT

```

Tue Jul 14 04:49:01
2009Z,WPCSvc,@%SystemRoot%\system32\wpcsvc.dll;-100,%SystemRoot%\system32\svchost.exe -k LocalServiceNetworkRestricted,,Manual,****NT Authority\LocalService
Tue Jul 14 04:49:01
2009Z,WPDBusEnum,@%SystemRoot%\system32\wpdbusenum.dll;-100,%SystemRoot%\system32\svchost.exe -k LocalSystemNetworkRestricted,,Manual,****LocalSystem
Tue Jul 14 04:49:01
2009Z,WPDBusEnum\Parameters,,%SystemRoot%\system32\wpdbusenum.dll,,,
Tue Jul 14 04:49:01
2009Z,wscsvc,@%SystemRoot%\System32\wscsvc.dll;-200,%SystemRoot%\System32\svchost.exe -k LocalServiceNetworkRestricted,,Auto Start,****NT AUTHORITY\LocalService
Tue Jul 14 04:49:01 2009Z,wscsvc\Parameters,,%SystemRoot%\System32\wscsvc.dll,,,
Tue Jul 14 04:49:01 2009Z,WSearchIdxPi,,,^^^^,,
Tue Jul 14 04:49:01 2009Z,wuauerv\Parameters,,%systemroot%\system32\wuaueng.dll,,,
Tue Jul 14 04:49:01 2009Z,wudfsvc\Parameters,,%SystemRoot%\System32\WUDFSvc.dll,,,
Tue Jul 14 04:49:01
2009Z,WwanSvc,@%SystemRoot%\System32\wwansvc.dll;-257,%SystemRoot%\system32\svchost.exe -k LocalServiceNoNetwork,,Manual,****NT Authority\LocalService
Tue Jul 14 04:49:01 2009Z,WwanSvc\Parameters,,%SystemRoot%\System32\wwansvc.dll,,,
Tue Jul 14 04:49:01 2009Z,xmprov,,,^^^^,,
Tue Jul 14 02:34:41 2009Z,DcomLaunch\Parameters,,%SystemRoot%\system32\rpcss.dll,,,
Tue Jul 14 02:34:41 2009Z,RpcSs\Parameters,,%SystemRoot%\system32\rpcss.dll,,,
-----

```

svcdll v.20130603

(System) Lists Services keys with ServiceDll values

Sun Feb 21 00:01:18 2016Z

WinDefend -> %ProgramFiles%\Windows Defender\mpsvc.dll

Wed Feb 3 04:32:57 2016Z

BITS -> %SystemRoot%\System32\qmgr.dll

Wed Nov 11 20:31:53 2015Z

SharedAccess -> %SystemRoot%\System32\ipnathlp.dll

Sat Sep 12 00:09:28 2015Z

stisvc -> %SystemRoot%\System32\wiaservc.dll

Fri Sep 11 07:47:27 2015Z

WbioSrv -> %SystemRoot%\System32\wbiosrv.dll

Thu Sep 10 20:46:43 2015Z

DiagTrack -> %SystemRoot%\system32\diagtrack.dll

Thu Sep 10 17:10:15 2015Z

IKEEXT -> %SystemRoot%\System32\ikeext.dll

Thu Sep 10 04:09:02 2015Z

## SYSTEM OUTPUT

HomeGroupListener -> %SystemRoot%\system32>ListSvc.dll

Thu Sep 10 04:08:46 2015Z  
FDResPub -> %SystemRoot%\system32\fdrespub.dll

Thu Sep 3 17:49:58 2015Z  
CertPropSvc -> %SystemRoot%\System32\certprop.dll  
SCardSvr -> %SystemRoot%\System32\SCardSvr.dll

Fri Feb 20 18:42:17 2015Z  
EapHost -> %SystemRoot%\System32\eapsvc.dll

Mon Dec 1 14:38:46 2014Z  
SysMain -> %systemroot%\system32\sysmain.dll

Mon Dec 1 14:14:27 2014Z  
gpsvc -> %SystemRoot%\System32\gpsvc.dll

Mon Dec 1 13:04:59 2014Z  
wuauerv -> %systemroot%\system32\wuaueng.dll

Mon Dec 1 12:59:19 2014Z  
Wlansvc -> %SystemRoot%\System32\wlansvc.dll

Sat Nov 29 16:11:45 2014Z  
WebClient -> %SystemRoot%\System32\webclnt.dll

Sat Nov 29 16:07:24 2014Z  
wudfsvc -> %SystemRoot%\System32\WUDFSvc.dll

Sat Nov 29 16:06:59 2014Z  
FontCache -> %SystemRoot%\system32\FntCache.dll

Tue Apr 12 08:29:05 2011Z  
CscService -> %SystemRoot%\System32\cscsvc.dll

Tue Apr 12 08:28:48 2011Z  
AppMgmt -> %SystemRoot%\System32\appmgmts.dll  
Mcx2Svc -> %SystemRoot%\system32\Mcx2Svc.dll  
PeerDistSvc -> %SystemRoot%\system32\peerdistsvc.dll  
SensrSvc -> %SystemRoot%\system32\sensrsvc.dll  
StorSvc -> %SystemRoot%\system32\storsvc.dll  
UmRdpService -> %SystemRoot%\System32\umrdp.dll

Sun Nov 21 03:33:56 2010Z  
SessionEnv -> %SystemRoot%\system32\sessenv.dll

Tue Jul 14 04:53:45 2009Z

## SYSTEM OUTPUT

TrkWks -> %SystemRoot%\System32\trkwks.dll

Tue Jul 14 04:53:36 2009Z  
RpcEptMapper -> %SystemRoot%\System32\RpcEpMap.dll

Tue Jul 14 04:53:33 2009Z  
LanmanServer -> %SystemRoot%\system32\svrsvcs.dll

Tue Jul 14 04:53:31 2009Z  
LanmanWorkstation -> %SystemRoot%\System32\wkssvc.dll

Tue Jul 14 04:53:24 2009Z  
Winmgmt -> %SystemRoot%\system32\wbem\WMIsvc.dll

Tue Jul 14 04:53:20 2009Z  
lmhosts -> %SystemRoot%\System32\lmhsvc.dll

Tue Jul 14 04:53:19 2009Z  
Dhcp -> %SystemRoot%\system32\dhcpcore.dll

Tue Jul 14 04:49:48 2009Z  
W32Time -> %systemroot%\system32\w32time.dll

Tue Jul 14 04:49:46 2009Z  
Dnscache -> %SystemRoot%\System32\dnsrslvr.dll

Tue Jul 14 04:49:45 2009Z  
RemoteAccess -> %SystemRoot%\System32\mprdim.dll

Tue Jul 14 04:49:35 2009Z  
RasAuto -> %SystemRoot%\System32\rasauto.dll  
RasMan -> %SystemRoot%\System32\rasmans.dll

Tue Jul 14 04:49:24 2009Z  
DPS -> %SystemRoot%\system32\dps.dll  
WdiServiceHost -> %SystemRoot%\system32\wdi.dll  
WdiSystemHost -> %SystemRoot%\system32\wdi.dll

Tue Jul 14 04:49:01 2009Z  
AeLookupSvc -> %SystemRoot%\System32\aelupsvc.dll  
AppIDSvc -> %SystemRoot%\System32\appidsvc.dll  
Appinfo -> %SystemRoot%\System32\appinfo.dll  
AudioEndpointBuilder -> %SystemRoot%\System32\Audiosrv.dll  
AudioSrv -> %SystemRoot%\System32\Audiosrv.dll  
AxInstSV -> %SystemRoot%\System32\AxInstSV.dll  
BDESVC -> %SystemRoot%\System32\bdesvc.dll  
BFE -> %SystemRoot%\System32\bfe.dll  
Browser -> %SystemRoot%\System32\browser.dll



## SYSTEM OUTPUT

bthserv -> %SystemRoot%\system32\bthserv.dll  
 CryptSvc -> %SystemRoot%\system32\cryptsvc.dll  
 DcomLaunch -> %SystemRoot%\system32\rpcss.dll  
 defragsvc -> %SystemRoot%\system32\defragsvc.dll  
 dot3svc -> %SystemRoot%\system32\dot3svc.dll  
 EventSystem -> %systemroot%\system32\es.dll  
 fdPHost -> %SystemRoot%\system32\fdPHost.dll  
 hidserv -> %SystemRoot%\system32\hidserv.dll  
 hkmsvc -> %SystemRoot%\system32\kmsvc.dll  
 HomeGroupProvider -> %SystemRoot%\system32\provsvc.dll  
 IPBusEnum -> %SystemRoot%\system32\ipbusenum.dll  
 iphlpsvc -> %SystemRoot%\system32\iphlpvc.dll  
 KtmRm -> %systemroot%\system32\msdtckrm.dll  
 lltdsvc -> %SystemRoot%\system32\lltdsvc.dll  
 MMCSS -> %SystemRoot%\system32\mmcscs.dll  
 MpsSvc -> %SystemRoot%\system32\mpssvc.dll  
 MSiSCSI -> %systemroot%\system32\iscsiexe.dll  
 napagent -> %SystemRoot%\system32\qagentRT.dll  
 Netman -> %SystemRoot%\system32\netman.dll  
 netprofm -> %SystemRoot%\system32\netprofm.dll  
 NlaSvc -> %SystemRoot%\system32\nlasvc.dll  
 nsi -> %systemroot%\system32\nsisvc.dll  
 p2pimsvc -> %SystemRoot%\system32\pnrpvc.dll  
 p2psvc -> %SystemRoot%\system32\p2psvc.dll  
 PcaSvc -> %SystemRoot%\system32\pcasvc.dll  
 pla -> %systemroot%\system32\pla.dll  
 PlugPlay -> %SystemRoot%\system32\umpnmgm.dll  
 PNRPAutoReg -> %SystemRoot%\system32\pnrpauto.dll  
 PNRPsvc -> %SystemRoot%\system32\pnrpvc.dll  
 PolicyAgent -> %SystemRoot%\system32\ipseccs.dll  
 Power -> %SystemRoot%\system32\umpo.dll  
 ProfSvc -> %systemroot%\system32\profsvc.dll  
 QWAVE -> %windir%\system32\qwave.dll  
 RemoteRegistry -> %SystemRoot%\system32\regsvc.dll  
 RpcSs -> %SystemRoot%\system32\rpcss.dll  
 Schedule -> %systemroot%\system32\schedsvc.dll  
 SCPolicySvc -> %SystemRoot%\system32\certprop.dll  
 SDRSVC -> %SystemRoot%\system32\SDRSVC.dll  
 seclogon -> %windir%\system32\seclogon.dll  
 SENS -> %SystemRoot%\system32\sens.dll  
 ShellHWDetection -> %SystemRoot%\system32\shsvcs.dll  
 sppuotify -> %SystemRoot%\system32\sppuotify.dll  
 SSDPSRV -> %SystemRoot%\system32\ssdpsrv.dll  
 SstpSvc -> %SystemRoot%\system32\sstpsvc.dll  
 swprv -> %SystemRoot%\system32\swprv.dll  
 TabletInputService -> %SystemRoot%\system32\TabSvc.dll  
 TapiSrv -> %SystemRoot%\system32\tapisrv.dll  
 TermService -> %SystemRoot%\system32\termsrv.dll

## SYSTEM OUTPUT

Themes -> %SystemRoot%\system32\themeservice.dll  
 THREADORDER -> %SystemRoot%\system32\mmcsm.dll  
 upnphost -> %SystemRoot%\System32\upnphost.dll  
 UxSms -> %SystemRoot%\System32\uxsms.dll  
 wcnscvc -> %SystemRoot%\System32\wcnscvc.dll  
 WcsPlugInService -> %SystemRoot%\System32\WcsPlugInService.dll  
 Wecsvc -> %SystemRoot%\system32\wecsvc.dll  
 wercplsupport -> %SystemRoot%\System32\wercplsupport.dll  
 WerSvc -> %SystemRoot%\System32\WerSvc.dll  
 WinHttpAutoProxySvc -> winhttp.dll  
 WinRM -> %SystemRoot%\system32\WsmSvc.dll  
 WPCSvc -> %SystemRoot%\System32\wpcsvc.dll  
 WPDBusEnum -> %SystemRoot%\system32\wpdbusenum.dll  
 wscsvc -> %SystemRoot%\System32\wscsvc.dll  
 WwanSvc -> %SystemRoot%\System32\wwansvc.dll

-----  
 ControlSet001\Control\Terminal Server  
 LastWrite Time Wed Apr 20 02:36:52 2016 (UTC)

Reference: <http://support.microsoft.com/kb/243215>

ProductVersion = 5.1

fDenyTSConnections = 1  
 1 = connections denied

TSAdvertise = 0  
 0 = disabled, 1 = enabled (advertise Terminal Services)  
 Ref: <http://support.microsoft.com/kb/281307>

TSUserEnabled = 0  
 1 = All users logging in are automatically part of the  
 built-in Terminal Server User group. 0 = No one is a  
 member of the built-in group.  
 Ref: <http://support.microsoft.com/kb/238965>

## AutoStart Locations

Wds\rdpwd key

StartupPrograms: rdpclip

Analysis Tip: This value usually contains 'rdpclip'; any additional entries  
 should be investigated.

WinStations\RDP-Tcp key

InitialProgram: {blank}

Analysis Tip: Maybe be empty; appears as '{blank}'

## SYSTEM OUTPUT

WinStations\RDP-Tcp key

UserAuthentication: 0

Analysis Tip: If the UserAuthentication value is 0, the system may be susceptible to a priv escalation exploitation via Sticky Keys. See: <http://www.room362.com/blog/2012/5/25/sticky-keys-and-utilman-against-nla.html>

-----  
timezone v.20130830

(System) Get TimeZoneInformation key contents

TimeZoneInformation key

ControlSet001\Control\TimeZoneInformation

LastWrite Time Sun Mar 13 09:56:24 2016 (UTC)

DaylightName -> @tzres.dll,-111

StandardName -> @tzres.dll,-112

Bias -> 300 (5 hours)

ActiveTimeBias -> 240 (4 hours)

-----  
usb v.20141111

(System) Get USB key info

USBStor

ControlSet001\Enum\USB

ROOT\_HUB20 [Mon Apr 18 00:13:48 2016]

S/N: 4&23d818d8&0 [Wed Apr 20 02:36:42 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

ParentIdPrefix: 5&1885ead0&0

InstallDate : Fri Feb 20 16:53:50 2015 UTC

FirstInstallDate: Fri Feb 20 16:53:50 2015 UTC

S/N: 4&2587f323&0 [Wed Apr 20 02:36:41 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

ParentIdPrefix: 5&22a566ae&0

InstallDate : Fri Feb 20 16:53:50 2015 UTC

FirstInstallDate: Fri Feb 20 16:53:50 2015 UTC

VID\_0000&PID\_0000 [Mon Apr 18 00:13:48 2016]

S/N: 6&1ce479a2&0&2 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

InstallDate : Thu Nov 19 17:59:30 2015 UTC

FirstInstallDate: Thu Nov 19 17:59:30 2015 UTC

## SYSTEM OUTPUT

VID\_03F0&PID\_0024 [Mon Apr 18 00:13:48 2016]  
 S/N: 7&7b672&0&2 [Wed Apr 20 02:36:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 8&17a24295&0  
 InstallDate : Wed Sep 16 04:53:56 2015 UTC  
 FirstInstallDate: Wed Sep 16 04:53:56 2015 UTC  
 S/N: 7&7b672&0&3 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 8&2a5bf33a&0  
 InstallDate : Sat Sep 12 16:08:21 2015 UTC  
 FirstInstallDate: Sat Sep 12 16:08:21 2015 UTC

VID\_03F0&PID\_0C4A [Mon Apr 18 00:13:48 2016]  
 S/N: 7&7b672&0&1 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 8&c13e7e8&0  
 InstallDate : Wed Sep 16 04:54:15 2015 UTC  
 FirstInstallDate: Wed Sep 16 04:54:15 2015 UTC  
 S/N: 7&7b672&0&4 [Wed Apr 20 02:36:49 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 8&f81a000&0  
 InstallDate : Thu Sep 10 17:02:33 2015 UTC  
 FirstInstallDate: Thu Sep 10 17:02:33 2015 UTC

VID\_03F0&PID\_231D [Mon Apr 18 00:13:48 2016]  
 S/N: 6&1ce479a2&0&6 [Wed Apr 20 02:36:49 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 7&2cb8892b&0  
 InstallDate : Fri Feb 20 16:54:12 2015 UTC  
 FirstInstallDate: Fri Feb 20 16:54:12 2015 UTC

VID\_03F0&PID\_B107 [Mon Apr 18 00:13:48 2016]  
 S/N: 002354D46B97AC5102CF01C0 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Sat Sep 12 01:43:16 2015 UTC  
 FirstInstallDate: Sat Sep 12 01:43:16 2015 UTC

## SYSTEM OUTPUT

VID\_0424&PID\_2514 [Mon Apr 18 00:13:48 2016]  
 S/N: 6&2a8ba21b&0&4 [Wed Apr 20 02:36:44 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 7&7b672&0  
 InstallDate : Thu Sep 10 17:02:38 2015 UTC  
 FirstInstallDate: Thu Sep 10 17:02:38 2015 UTC

VID\_04F2&PID\_B230 [Mon Apr 18 00:13:48 2016]  
 S/N: SN0001 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 7&369e123a&0  
 InstallDate : Fri Feb 20 16:54:11 2015 UTC  
 FirstInstallDate: Fri Feb 20 16:54:11 2015 UTC

VID\_04F2&PID\_B230&MI\_00 [Mon Apr 18 00:13:48 2016]  
 S/N: 7&369e123a&0&0000 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : HP HD Webcam [Fixed]  
 InstallDate : Fri Feb 20 16:54:13 2015 UTC  
 FirstInstallDate: Fri Feb 20 16:54:13 2015 UTC

VID\_04F9&PID\_02B0 [Mon Apr 18 00:13:48 2016]  
 S/N: U63481G5J873107 [Wed Apr 20 02:36:49 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 9&13a85fb5&0  
 InstallDate : Tue Feb 2 00:10:51 2016 UTC  
 FirstInstallDate: Tue Feb 2 00:10:51 2016 UTC

VID\_04F9&PID\_02B0&MI\_00 [Mon Apr 18 00:13:48 2016]  
 S/N: 9&13a85fb5&0&0000 [Wed Apr 20 02:36:49 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: a&9fb95b6&0  
 InstallDate : Tue Feb 2 00:16:45 2016 UTC  
 FirstInstallDate: Tue Feb 2 00:16:45 2016 UTC

VID\_04F9&PID\_02B0&MI\_01 [Mon Apr 18 00:13:48 2016]  
 S/N: 9&13a85fb5&0&0001 [Wed Apr 20 02:36:49 2016]

## SYSTEM OUTPUT

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Tue Feb 2 00:28:11 2016 UTC  
 FirstInstallDate: Tue Feb 2 00:11:45 2016 UTC

VID\_04F9&PID\_02B0&MI\_02 [Mon Apr 18 00:13:48 2016]  
 S/N: 9&13a85fb5&0&0002 [Wed Apr 20 02:36:49 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : Brother MFC-9340CDW Remote Setup Port (COM5)  
 InstallDate : Tue Feb 2 00:29:07 2016 UTC  
 FirstInstallDate: Tue Feb 2 00:16:42 2016 UTC

VID\_054C&PID\_06F0 [Mon Apr 18 00:13:48 2016]  
 S/N: C68B200FB019 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Fri Nov 20 01:55:51 2015 UTC  
 FirstInstallDate: Fri Nov 20 01:55:51 2015 UTC

VID\_054C&PID\_0830 [Mon Apr 18 00:13:48 2016]  
 S/N: C68B200FB019 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 7&18ddaeb8&0  
 InstallDate : Fri Oct 2 22:37:51 2015 UTC  
 FirstInstallDate: Fri Oct 2 22:37:51 2015 UTC

VID\_058F&PID\_9540 [Mon Apr 18 00:13:48 2016]  
 S/N: 6&1ce479a2&0&8 [Wed Apr 20 02:36:48 2016]  
 Device Parameters LastWrite: [Wed Apr 20 02:37:07 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 7&22546dd0&0  
 InstallDate : Thu Sep 3 17:49:59 2015 UTC  
 FirstInstallDate: Thu Sep 3 17:49:59 2015 UTC

VID\_05AC&PID\_1281 [Mon Apr 18 00:13:48 2016]  
 S/N:  
 CPID:7000\_CPRV:11\_CPFM:03\_SCEP:01\_BDID:06\_ECID:000E485A0845A426\_IBFL:1C\_SRMN:[F1FPTK  
 22G5MF] [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]

## SYSTEM OUTPUT

FriendlyName : @oem45.inf,%iPhone.DeviceDesc%;Apple Mobile Device USB Driver  
 InstallDate : Sat Feb 20 01:01:39 2016 UTC  
 FirstInstallDate: Sat Feb 20 01:01:39 2016 UTC

S/N:

CPID:7000\_CPRV:11\_CPFM:03\_SCEP:01\_BDID:06\_ECID:000E485A0845A426\_IBFL:1D\_SRMN:[F1FPTK  
 22G5MF] [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

FriendlyName : @oem45.inf,%iPhone.DeviceDesc%;Apple Mobile Device USB Driver  
 InstallDate : Sat Feb 20 01:01:30 2016 UTC  
 FirstInstallDate: Sat Feb 20 01:01:30 2016 UTC

VID\_05AC&PID\_12A8 [Mon Apr 18 00:13:48 2016]

S/N: 240d1c4b911b3a8be55e1bf21356bcae6fa0ec28 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

FriendlyName : @oem45.inf,%iPhone.DeviceDesc%;Apple Mobile Device USB Driver  
 InstallDate : Thu Sep 24 18:58:32 2015 UTC  
 FirstInstallDate: Thu Sep 24 18:58:32 2015 UTC

S/N: 61bb57c4b96e289fcb630a41e840a255c7518299 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

FriendlyName : @oem45.inf,%iPhone.DeviceDesc%;Apple Mobile Device USB Driver  
 InstallDate : Thu Sep 24 22:59:55 2015 UTC  
 FirstInstallDate: Thu Sep 24 22:59:55 2015 UTC

VID\_05AC&PID\_12A8&MI\_00 [Mon Apr 18 00:13:48 2016]

S/N: 0 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

FriendlyName : Apple iPhone  
 InstallDate : Thu Sep 24 18:59:57 2015 UTC  
 FirstInstallDate: Thu Sep 24 18:59:57 2015 UTC

VID\_05AC&PID\_12A8&MI\_02 [Mon Apr 18 00:13:48 2016]

S/N: 2 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

InstallDate : Sat Nov 28 20:21:45 2015 UTC  
 FirstInstallDate: Sat Nov 28 20:21:45 2015 UTC

VID\_05AC&PID\_1301 [Mon Apr 18 00:13:48 2016]

S/N: 000A27001CA9A995 [Mon Apr 18 00:13:48 2016]

## SYSTEM OUTPUT

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Thu Nov 19 17:47:55 2015 UTC  
 FirstInstallDate: Thu Nov 19 17:47:55 2015 UTC

VID\_0718&PID\_0111 [Mon Apr 18 00:13:48 2016]  
 S/N: 0718011120035AF [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Mon Oct 19 13:06:12 2015 UTC  
 FirstInstallDate: Mon Oct 19 13:06:12 2015 UTC

VID\_0781&PID\_5151 [Mon Apr 18 00:13:48 2016]  
 S/N: 2243400CB8E0533D [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Wed Apr 6 14:24:53 2016 UTC  
 FirstInstallDate: Wed Apr 6 14:24:53 2016 UTC

VID\_0781&PID\_5530 [Mon Apr 18 00:13:48 2016]  
 S/N: 17380302D5A10198 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Fri Feb 20 17:01:42 2015 UTC  
 FirstInstallDate: Fri Feb 20 17:01:42 2015 UTC  
 S/N: 200544568018E7B0762E [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Mon Oct 26 09:55:43 2015 UTC  
 FirstInstallDate: Mon Oct 26 09:55:43 2015 UTC

VID\_091E&PID\_455B [Mon Apr 18 00:13:48 2016]  
 S/N: 0000e763bae0 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : nüvi 2555  
 InstallDate : Sat Sep 12 00:09:30 2015 UTC  
 FirstInstallDate: Sat Sep 12 00:09:30 2015 UTC

VID\_0BC2&PID\_3008 [Mon Apr 18 00:13:48 2016]  
 S/N: 2GEYC3F8 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]



## SYSTEM OUTPUT

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Sat Dec 12 12:37:50 2015 UTC  
 FirstInstallDate: Sat Dec 12 12:37:50 2015 UTC

VID\_0BC2&PID\_AB24 [Mon Apr 18 00:13:48 2016]

S/N: NA76YAT8 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Thu Sep 10 17:14:09 2015 UTC  
 FirstInstallDate: Thu Sep 10 17:14:09 2015 UTC

VID\_0D8C&PID\_0005 [Mon Apr 18 00:13:48 2016]

S/N: 201510 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 7&307cc9e2&0  
 InstallDate : Sun Feb 14 15:56:12 2016 UTC  
 FirstInstallDate: Sun Feb 14 15:56:12 2016 UTC

VID\_0D8C&PID\_0005&MI\_00 [Mon Apr 18 00:13:48 2016]

S/N: 7&307cc9e2&0&0000 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : Blue Snowball  
 InstallDate : Sun Feb 14 15:57:33 2016 UTC  
 FirstInstallDate: Sun Feb 14 15:57:33 2016 UTC

VID\_0D8C&PID\_0005&MI\_02 [Mon Apr 18 00:13:48 2016]

S/N: 7&307cc9e2&0&0002 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 8&39aa15e6&0  
 InstallDate : Sun Feb 14 15:56:39 2016 UTC  
 FirstInstallDate: Sun Feb 14 15:56:39 2016 UTC

VID\_138A&PID\_003C [Mon Apr 18 00:13:48 2016]

S/N: 0020c01ba98d [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : @oem30.inf,%FriendlyName%;Validity Sensor  
 InstallDate : Fri Feb 20 18:22:44 2015 UTC  
 FirstInstallDate: Fri Feb 20 18:22:44 2015 UTC

## SYSTEM OUTPUT

S/N: 00a0cc7ef68b [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : @oem30.inf,%FriendlyName%;Validity Sensor  
 InstallDate : Fri Feb 20 17:05:33 2015 UTC  
 FirstInstallDate: Fri Feb 20 16:54:12 2015 UTC

VID\_13FE&PID\_3600 [Mon Apr 18 00:13:48 2016]  
 S/N: 07032B5A180AA664 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Mon Sep 14 18:39:03 2015 UTC  
 FirstInstallDate: Mon Sep 14 18:39:03 2015 UTC

VID\_13FE&PID\_4200 [Mon Apr 18 00:13:48 2016]  
 S/N: 070B43D2DE271C28 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Thu Oct 1 23:47:37 2015 UTC  
 FirstInstallDate: Thu Oct 1 23:47:37 2015 UTC  
 S/N: 070B43D9AB6E9253 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Sat Mar 19 22:25:23 2016 UTC  
 FirstInstallDate: Sat Mar 19 22:25:23 2016 UTC

VID\_154B&PID\_0059 [Mon Apr 18 00:13:48 2016]  
 S/N: AABA1ECC00001167 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Mon Oct 19 13:06:26 2015 UTC  
 FirstInstallDate: Mon Oct 19 13:06:26 2015 UTC

VID\_154B&PID\_005B [Mon Apr 18 00:13:48 2016]  
 S/N: ACB3HD1000000240 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Thu Oct 8 00:17:51 2015 UTC  
 FirstInstallDate: Thu Oct 8 00:17:51 2015 UTC

VID\_1A40&PID\_0101 [Mon Apr 18 00:13:48 2016]  
 S/N: 7&7b672&0&3 [Wed Apr 20 02:36:49 2016]

## SYSTEM OUTPUT

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Wed Sep 23 03:07:47 2015 UTC  
 FirstInstallDate: Wed Sep 23 03:07:47 2015 UTC

VID\_1BCF&PID\_2888 [Mon Apr 18 00:13:48 2016]  
 S/N: 6&1ce479a2&0&4 [Wed Apr 20 02:36:46 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 7&4e0c875&0  
 InstallDate : Thu Sep 3 17:50:00 2015 UTC  
 FirstInstallDate: Thu Sep 3 17:50:00 2015 UTC

VID\_1BCF&PID\_2888&MI\_00 [Mon Apr 18 00:13:48 2016]  
 S/N: 7&4e0c875&0&0000 [Wed Apr 20 02:36:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : @oem51.inf,%SPUVCB.Capture%;HP HD Webcam [Fixed]  
 InstallDate : Wed Sep 23 14:01:33 2015 UTC  
 FirstInstallDate: Thu Sep 3 17:50:03 2015 UTC

VID\_1C4F&PID\_0002 [Mon Apr 18 00:13:48 2016]  
 S/N: 7&7b672&0&3 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 8&1617e4af&0  
 InstallDate : Thu Sep 10 17:02:40 2015 UTC  
 FirstInstallDate: Thu Sep 10 17:02:40 2015 UTC

VID\_1C4F&PID\_0002&MI\_00 [Mon Apr 18 00:13:48 2016]  
 S/N: 8&1617e4af&0&0000 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 9&20bb9c62&0  
 InstallDate : Thu Sep 10 17:02:42 2015 UTC  
 FirstInstallDate: Thu Sep 10 17:02:42 2015 UTC

VID\_1C4F&PID\_0002&MI\_01 [Mon Apr 18 00:13:48 2016]  
 S/N: 8&1617e4af&0&0001 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 9&8f8101d&0

## SYSTEM OUTPUT

InstallDate : Thu Sep 10 17:02:41 2015 UTC  
 FirstInstallDate: Thu Sep 10 17:02:41 2015 UTC

VID\_2687&PID\_FB01 [Mon Apr 18 00:13:48 2016]  
 S/N: 6&1ce479a2&0&2 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 7&23a259f1&0  
 InstallDate : Sat Nov 28 19:56:09 2015 UTC  
 FirstInstallDate: Sat Nov 28 19:56:09 2015 UTC  
 S/N: 6&282d7f15&0&3 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 7&d4af04&0  
 InstallDate : Thu Jan 14 21:58:50 2016 UTC  
 FirstInstallDate: Thu Jan 14 21:58:50 2016 UTC

VID\_2687&PID\_FB01&MI\_00 [Mon Apr 18 00:13:48 2016]  
 S/N: 7&23a259f1&0&0000 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 8&1a44e8e&0  
 InstallDate : Sat Nov 28 19:56:41 2015 UTC  
 FirstInstallDate: Sat Nov 28 19:56:41 2015 UTC  
 S/N: 7&d4af04&0&0000 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 8&41a69fc&0  
 InstallDate : Thu Jan 14 21:59:00 2016 UTC  
 FirstInstallDate: Thu Jan 14 21:59:00 2016 UTC

VID\_2687&PID\_FB01&MI\_01 [Mon Apr 18 00:13:48 2016]  
 S/N: 7&23a259f1&0&0001 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 8&1967dad3&0  
 InstallDate : Sat Nov 28 19:58:07 2015 UTC  
 FirstInstallDate: Sat Nov 28 19:58:07 2015 UTC  
 S/N: 7&d4af04&0&0001 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 8&3ad05607&0

## SYSTEM OUTPUT

InstallDate : Thu Jan 14 21:59:49 2016 UTC  
 FirstInstallDate: Thu Jan 14 21:59:49 2016 UTC

VID\_0087&PID\_0024 [Mon Apr 18 00:13:48 2016]  
 S/N: 5&1885ead0&0&1 [Wed Apr 20 02:36:43 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 6&1ce479a2&0  
 InstallDate : Fri Feb 20 16:54:09 2015 UTC  
 FirstInstallDate: Fri Feb 20 16:54:09 2015 UTC  
 S/N: 5&22a566ae&0&1 [Wed Apr 20 02:36:43 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 ParentIdPrefix: 6&2a8ba21b&0  
 InstallDate : Fri Feb 20 16:54:10 2015 UTC  
 FirstInstallDate: Fri Feb 20 16:54:10 2015 UTC

-----  
 usbdevices v.20140416

(System) Parses Enum\USB key for USB & WPD devices

VID\_03F0&PID\_B107  
 LastWrite: Mon Apr 18 00:13:48 2016  
 SN : 002354D46B97AC5102CF01C0  
 LastWrite: Mon Apr 18 00:13:48 2016

VID\_054C&PID\_06F0  
 LastWrite: Mon Apr 18 00:13:48 2016  
 SN : C68B200FB019  
 LastWrite: Mon Apr 18 00:13:48 2016

VID\_05AC&PID\_12A8&MI\_00  
 LastWrite: Mon Apr 18 00:13:48 2016  
 SN : 0  
 LastWrite: Mon Apr 18 00:13:48 2016  
 MFG : Apple Inc.  
 FriendlyName: Apple iPhone

VID\_05AC&PID\_1301  
 LastWrite: Mon Apr 18 00:13:48 2016  
 SN : 000A27001CA9A995  
 LastWrite: Mon Apr 18 00:13:48 2016

VID\_0718&PID\_0111  
 LastWrite: Mon Apr 18 00:13:48 2016  
 SN : 0718011120035AF

) Page 333

## SYSTEM OUTPUT

LastWrite: Mon Apr 18 00:13:48 2016

VID\_0781&PID\_5151

LastWrite: Mon Apr 18 00:13:48 2016

SN : 2243400CB8E0533D

LastWrite: Mon Apr 18 00:13:48 2016

VID\_0781&PID\_5530

LastWrite: Mon Apr 18 00:13:48 2016

SN : 17380302D5A10198

LastWrite: Mon Apr 18 00:13:48 2016

VID\_0781&PID\_5530

LastWrite: Mon Apr 18 00:13:48 2016

SN : 200544568018E7B0762E

LastWrite: Mon Apr 18 00:13:48 2016

VID\_091E&PID\_455B

LastWrite: Mon Apr 18 00:13:48 2016

SN : 0000e763bae0

LastWrite: Mon Apr 18 00:13:48 2016

MFG : Garmin

FriendlyName: nüvi 2555

VID\_0BC2&PID\_3008

LastWrite: Mon Apr 18 00:13:48 2016

SN : 2GEYC3F8\_\_\_\_\_

LastWrite: Mon Apr 18 00:13:48 2016

VID\_0BC2&PID\_AB24

LastWrite: Mon Apr 18 00:13:48 2016

SN : NA76YAT8

LastWrite: Mon Apr 18 00:13:48 2016

VID\_13FE&PID\_3600

LastWrite: Mon Apr 18 00:13:48 2016

SN : 07032B5A180AA664

LastWrite: Mon Apr 18 00:13:48 2016

VID\_13FE&PID\_4200

LastWrite: Mon Apr 18 00:13:48 2016

SN : 070B43D2DE271C28

LastWrite: Mon Apr 18 00:13:48 2016

VID\_13FE&PID\_4200

LastWrite: Mon Apr 18 00:13:48 2016

SN : 070B43D9AB6E9253

LastWrite: Mon Apr 18 00:13:48 2016

## SYSTEM OUTPUT

VID\_154B&amp;PID\_0059

LastWrite: Mon Apr 18 00:13:48 2016

SN : AABA1ECC00001167

LastWrite: Mon Apr 18 00:13:48 2016

VID\_154B&amp;PID\_005B

LastWrite: Mon Apr 18 00:13:48 2016

SN : ACB3HD1000000240

LastWrite: Mon Apr 18 00:13:48 2016

-----  
usbstor v.20141111

(System) Get USBStor key info

USBStor

ControlSet001\Enum\USBStor

Disk&amp;Ven\_&amp;Prod\_&amp;Rev\_2.20 [Mon Apr 18 00:13:48 2016]

S/N: 0718011120035AF&amp;0 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

FriendlyName : USB Device

InstallDate : Mon Oct 19 13:06:14 2015 UTC

FirstInstallDate: Mon Oct 19 13:06:14 2015 UTC

Disk&amp;Ven\_&amp;Prod\_&amp;Rev\_PMAP [Mon Apr 18 00:13:48 2016]

S/N: 07032B5A180AA664&amp;0 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

FriendlyName : USB Device

InstallDate : Mon Sep 14 18:39:05 2015 UTC

FirstInstallDate: Mon Sep 14 18:39:05 2015 UTC

S/N: 070B43D2DE271C28&amp;0 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

FriendlyName : USB Device

InstallDate : Thu Oct 1 23:47:40 2015 UTC

FirstInstallDate: Thu Oct 1 23:47:40 2015 UTC

S/N: 070B43D9AB6E9253&amp;0 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

FriendlyName : USB Device

InstallDate : Sat Mar 19 22:25:24 2016 UTC

## SYSTEM OUTPUT

FirstInstallDate: Sat Mar 19 22:25:24 2016 UTC

Disk&Ven\_Apple&Prod\_iPod&Rev\_2.70 [Mon Apr 18 00:13:48 2016]

S/N: 000A27001CA9A995&0 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

FriendlyName : Apple iPod USB Device

InstallDate : Thu Nov 19 17:47:58 2015 UTC

FirstInstallDate: Thu Nov 19 17:47:58 2015 UTC

Disk&Ven\_hp&Prod\_USB\_FLASH\_DRIVE&Rev\_1.00 [Mon Apr 18 00:13:48 2016]

S/N: 002354D46B97AC5102CF01C0&0 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

FriendlyName : hp USB FLASH DRIVE USB Device

InstallDate : Sat Sep 12 01:43:20 2015 UTC

FirstInstallDate: Sat Sep 12 01:43:20 2015 UTC

Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_1100 [Mon Apr 18 00:13:48 2016]

S/N: ACB3HD1000000240&0 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

FriendlyName : PNY USB 2.0 FD USB Device

InstallDate : Thu Oct 8 00:17:54 2015 UTC

FirstInstallDate: Thu Oct 8 00:17:54 2015 UTC

Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_8192 [Mon Apr 18 00:13:48 2016]

S/N: AABA1ECC00001167&0 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

FriendlyName : PNY USB 2.0 FD USB Device

InstallDate : Mon Oct 19 13:06:27 2015 UTC

FirstInstallDate: Mon Oct 19 13:06:27 2015 UTC

Disk&Ven\_SanDisk&Prod\_Cruzer&Rev\_1.20 [Mon Apr 18 00:13:48 2016]

S/N: 200544568018E7B0762E&0 [Mon Apr 18 00:13:48 2016]

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

FriendlyName : SanDisk Cruzer USB Device

InstallDate : Mon Oct 26 09:55:50 2015 UTC

FirstInstallDate: Mon Oct 26 09:55:50 2015 UTC

Disk&Ven\_SanDisk&Prod\_Cruzer&Rev\_8.02 [Mon Apr 18 00:13:48 2016]



## SYSTEM OUTPUT

S/N: 17380302D5A10198&0 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : SanDisk Cruzer USB Device  
 InstallDate : Fri Feb 20 17:01:43 2015 UTC  
 FirstInstallDate: Fri Feb 20 17:01:43 2015 UTC

Disk&Ven\_SanDisk&Prod\_Cruzer\_Micro&Rev\_8.02 [Mon Apr 18 00:13:48 2016]

S/N: 2243400CB8E0533D&0 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : SanDisk Cruzer Micro USB Device  
 InstallDate : Wed Apr 6 14:25:00 2016 UTC  
 FirstInstallDate: Wed Apr 6 14:25:00 2016 UTC

Disk&Ven\_Seagate&Prod\_BUP\_Slim\_SL&Rev\_0302 [Mon Apr 18 00:13:48 2016]

S/N: NA76YAT8&0 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : Seagate BUP Slim SL USB Device  
 InstallDate : Thu Sep 10 17:14:12 2015 UTC  
 FirstInstallDate: Thu Sep 10 17:14:12 2015 UTC

Disk&Ven\_Seagate&Prod\_FreeAgent&Rev\_0132 [Mon Apr 18 00:13:48 2016]

S/N: 2GEYC3F8\_\_\_\_&0 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : Seagate FreeAgent USB Device  
 InstallDate : Sat Dec 12 12:37:53 2015 UTC  
 FirstInstallDate: Sat Dec 12 12:37:53 2015 UTC

Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00 [Mon Apr 18 00:13:48 2016]

S/N: C68B200FB019&0 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : Sony DSC USB Device  
 InstallDate : Fri Nov 20 01:55:53 2015 UTC  
 FirstInstallDate: Fri Nov 20 01:55:53 2015 UTC  
 S/N: C68B200FB019&1 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : Sony DSC USB Device

## SYSTEM OUTPUT

InstallDate : Fri Nov 20 01:55:54 2015 UTC  
 FirstInstallDate: Fri Nov 20 01:55:54 2015 UTC  
 S/N: C68B200FB019&2 [Mon Apr 18 00:13:48 2016]  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 FriendlyName : Sony DSC USB Device  
 InstallDate : Fri Nov 20 01:55:52 2015 UTC  
 FirstInstallDate: Fri Nov 20 01:55:52 2015 UTC

-----  
 ABE-ARJUNMALIK,Disk&Ven\_&Prod\_&Rev\_2.20,0718011120035AF&0,1460938428,USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_&Prod\_&Rev\_PMAP,07032B5A180AA664&0,1460938428,USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_&Prod\_&Rev\_PMAP,070B43D2DE271C28&0,1460938428,USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_&Prod\_&Rev\_PMAP,070B43D9AB6E9253&0,1460938428,USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_Apple&Prod\_iPod&Rev\_2.70,000A27001CA9A995&0,1460938428,Apple iPod USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_hp&Prod\_USB\_FLASH\_DRIVE&Rev\_1.00,002354D46B97AC5102CF01C0&0,1460938428,hp USB FLASH DRIVE USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_1100,ACB3HD1000000240&0,1460938428,P NY USB 2.0 FD USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_8192,AABA1ECC00001167&0,1460938428,P NY USB 2.0 FD USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_SanDisk&Prod\_Cruzer&Rev\_1.20,200544568018E7B0762E&0,1460938428,SanDisk Cruzer USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_SanDisk&Prod\_Cruzer&Rev\_8.02,17380302D5A10198&0,1460938428,SanDisk Cruzer USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_SanDisk&Prod\_Cruzer\_Micro&Rev\_8.02,2243400CB8E0533D&0,1460938428,SanDisk Cruzer Micro USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_Seagate&Prod\_BUP\_Slim\_SL&Rev\_0302,NA76YAT8&0,1460938428,Seagate BUP Slim SL USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_Seagate&Prod\_FreeAgent&Rev\_0132,2GEYC3F8\_\_\_\_&0,1460938428,Seagate FreeAgent USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00,C68B200FB019&0,1460938428,Sony DSC USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00,C68B200FB019&1,1460938428,Sony DSC USB Device  
 ABE-ARJUNMALIK,Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00,C68B200FB019&2,1460938428,Sony DSC USB Device

-----  
 Disk&Ven\_&Prod\_&Rev\_2.20,Mon Apr 18 00:13:48 2016,0718011120035AF&0,Mon Apr 18 00:13:48 2016,USB Device,  
 Disk&Ven\_&Prod\_&Rev\_PMAP,Mon Apr 18 00:13:48 2016,07032B5A180AA664&0,Mon Apr 18 00:13:48 2016,USB Device,  
 Disk&Ven\_&Prod\_&Rev\_PMAP,Mon Apr 18 00:13:48 2016,070B43D2DE271C28&0,Mon Apr 18 00:13:48 2016,USB Device,  
 Disk&Ven\_&Prod\_&Rev\_PMAP,Mon Apr 18 00:13:48 2016,070B43D9AB6E9253&0,Mon Apr 18 00:13:48 2016,USB Device,

## SYSTEM OUTPUT

Disk&Ven\_Apple&Prod\_iPod&Rev\_2.70,Mon Apr 18 00:13:48 2016,000A27001CA9A995&0,Mon  
 Apr 18 00:13:48 2016,Apple iPod USB Device,  
 Disk&Ven\_hp&Prod\_USB\_FLASH\_DRIVE&Rev\_1.00,Mon Apr 18 00:13:48  
 2016,002354D46B97AC5102CF01C0&0,Mon Apr 18 00:13:48 2016,hp USB FLASH DRIVE USB  
 Device,  
 Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_1100,Mon Apr 18 00:13:48  
 2016,ACB3HD1000000240&0,Mon Apr 18 00:13:48 2016,PNY USB 2.0 FD USB Device,  
 Disk&Ven\_PNY&Prod\_USB\_2.0\_FD&Rev\_8192,Mon Apr 18 00:13:48  
 2016,AABA1ECC00001167&0,Mon Apr 18 00:13:48 2016,PNY USB 2.0 FD USB Device,  
 Disk&Ven\_SanDisk&Prod\_Cruzer&Rev\_1.20,Mon Apr 18 00:13:48  
 2016,200544568018E7B0762E&0,Mon Apr 18 00:13:48 2016,SanDisk Cruzer USB Device,  
 Disk&Ven\_SanDisk&Prod\_Cruzer&Rev\_8.02,Mon Apr 18 00:13:48  
 2016,17380302D5A10198&0,Mon Apr 18 00:13:48 2016,SanDisk Cruzer USB Device,  
 Disk&Ven\_SanDisk&Prod\_Cruzer\_Micro&Rev\_8.02,Mon Apr 18 00:13:48  
 2016,2243400CB8E0533D&0,Mon Apr 18 00:13:48 2016,SanDisk Cruzer Micro USB Device,  
 Disk&Ven\_Seagate&Prod\_BUP\_Slim\_SL&Rev\_0302,Mon Apr 18 00:13:48 2016,NA76YAT8&0,Mon  
 Apr 18 00:13:48 2016,Seagate BUP Slim SL USB Device,  
 Disk&Ven\_Seagate&Prod\_FreeAgent&Rev\_0132,Mon Apr 18 00:13:48 2016,2GEYC3F8\_\_\_\_&0,Mon  
 Apr 18 00:13:48 2016,Seagate FreeAgent USB Device,  
 Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00,Mon Apr 18 00:13:48 2016,C68B200FB019&0,Mon Apr 18  
 00:13:48 2016,Sony DSC USB Device,  
 Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00,Mon Apr 18 00:13:48 2016,C68B200FB019&1,Mon Apr 18  
 00:13:48 2016,Sony DSC USB Device,  
 Disk&Ven\_Sony&Prod\_DSC&Rev\_1.00,Mon Apr 18 00:13:48 2016,C68B200FB019&2,Mon Apr 18  
 00:13:48 2016,Sony DSC USB Device,

-----  
 xpedition v.20120722

(System) Queries System hive for XP Edition info

xpedition v.20120722

-----  
 wpdbusenum v.20141111

(System) Get WpdBusEnumRoot subkey info

DISK&VEN\_JMCR&PROD\_SD&REV\_ (5&12E35340&0&000000)

LastWrite: Mon Apr 18 00:13:48 2016

DeviceDesc: SD

Friendly: F:\

Mfg: JMCR

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

InstallDate : Wed Sep 23 03:08:51 2015 UTC

FirstInstallDate: Wed Sep 23 03:08:51 2015 UTC

DISK&VEN\_&PROD\_&REV\_2.20 (0718011120035AF&0)

LastWrite: Mon Apr 18 00:13:48 2016

DeviceDesc: @wpdfs.inf,%basicdevicename%;WPD FileSystem Volume Driver

## SYSTEM OUTPUT

Friendly: E:\

Mfg:

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

InstallDate : Mon Oct 19 13:06:21 2015 UTC

FirstInstallDate: Mon Oct 19 13:06:21 2015 UTC

DISK&VEN\_&PROD\_&REV\_PMAP (07032B5A180AA664&0)

LastWrite: Mon Apr 18 00:13:48 2016

DeviceDesc:

Friendly: THUMBDRIVE

Mfg:

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

InstallDate : Mon Sep 14 18:39:12 2015 UTC

FirstInstallDate: Mon Sep 14 18:39:12 2015 UTC

DISK&VEN\_&PROD\_&REV\_PMAP (070B43D2DE271C28&0)

LastWrite: Mon Apr 18 00:13:48 2016

DeviceDesc:

Friendly: USB DISK

Mfg:

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

InstallDate : Thu Oct 1 23:47:50 2015 UTC

FirstInstallDate: Thu Oct 1 23:47:50 2015 UTC

DISK&VEN\_&PROD\_&REV\_PMAP (070B43D9AB6E9253&0)

LastWrite: Mon Apr 18 00:13:48 2016

DeviceDesc:

Friendly: USB DISK

Mfg:

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

InstallDate : Sat Mar 19 22:25:28 2016 UTC

FirstInstallDate: Sat Mar 19 22:25:28 2016 UTC

DISK&VEN\_APPLE&PROD\_IPOD&REV\_2.70 (000A27001CA9A995&0)

LastWrite: Mon Apr 18 00:13:48 2016

DeviceDesc: iPod

Friendly: ABE-ARJUN M

Mfg: Apple

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

## SYSTEM OUTPUT

Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Thu Nov 19 17:48:07 2015 UTC  
 FirstInstallDate: Thu Nov 19 17:48:07 2015 UTC

## DISK&amp;VEN\_HP&amp;PROD\_USB\_FLASH\_DRIVE&amp;REV\_1.00 (002354D46B97AC5102CF01C0&amp;0)

LastWrite: Mon Apr 18 00:13:48 2016  
 DeviceDesc: USB FLASH DRIVE  
 Friendly: ITUNES  
 Mfg: hp  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Sat Sep 12 01:43:29 2015 UTC  
 FirstInstallDate: Sat Sep 12 01:43:29 2015 UTC

## DISK&amp;VEN\_PNY&amp;PROD\_USB\_2.0\_FD&amp;REV\_1100 (ACB3HD1000000240&amp;0)

LastWrite: Mon Apr 18 00:13:48 2016  
 DeviceDesc: USB 2.0 FD  
 Friendly: PHOTOS  
 Mfg: PNY  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Thu Oct 8 00:18:02 2015 UTC  
 FirstInstallDate: Thu Oct 8 00:18:02 2015 UTC

## DISK&amp;VEN\_PNY&amp;PROD\_USB\_2.0\_FD&amp;REV\_8192 (AABA1ECC00001167&amp;0)

LastWrite: Mon Apr 18 00:13:48 2016  
 DeviceDesc: USB 2.0 FD  
 Friendly: USB20FD  
 Mfg: PNY  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Mon Oct 19 13:06:32 2015 UTC  
 FirstInstallDate: Mon Oct 19 13:06:32 2015 UTC

## DISK&amp;VEN\_SANDISK&amp;PROD\_CRUZER&amp;REV\_1.20 (200544568018E7B0762E&amp;0)

LastWrite: Mon Apr 18 00:13:48 2016  
 DeviceDesc: Cruzer  
 Friendly: F:\  
 Mfg: SanDisk  
 Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]  
 LogConf LastWrite : [Mon Apr 18 00:13:48 2016]  
 Properties LastWrite : [Mon Apr 18 00:13:48 2016]  
 InstallDate : Mon Oct 26 09:56:14 2015 UTC  
 FirstInstallDate: Mon Oct 26 09:56:14 2015 UTC

## SYSTEM OUTPUT

DISK&VEN\_SANDISK&PROD\_CRUZER&REV\_8.02 (17380302D5A10198&0)

LastWrite: Mon Apr 18 00:13:48 2016

DeviceDesc: Cruzer

Friendly: F:\

Mfg: SanDisk

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:48 2016]

InstallDate : Fri Feb 20 17:01:44 2015 UTC

FirstInstallDate: Fri Feb 20 17:01:44 2015 UTC

DISK&VEN\_SANDISK&PROD\_CRUZER\_MICRO&REV\_8.02 (2243400CB8E0533D&0)

LastWrite: Mon Apr 18 00:13:49 2016

DeviceDesc: Cruzer Micro

Friendly: F:\

Mfg: SanDisk

Device Parameters LastWrite: [Mon Apr 18 00:13:48 2016]

LogConf LastWrite : [Mon Apr 18 00:13:48 2016]

Properties LastWrite : [Mon Apr 18 00:13:49 2016]

InstallDate : Wed Apr 6 14:25:07 2016 UTC

FirstInstallDate: Wed Apr 6 14:25:07 2016 UTC

DISK&VEN\_SONY&PROD\_DSC&REV\_1.00 (C68B200FB019&0)

LastWrite: Mon Apr 18 00:13:49 2016

DeviceDesc: DSC

Friendly: G:\

Mfg: Sony

Device Parameters LastWrite: [Mon Apr 18 00:13:49 2016]

LogConf LastWrite : [Mon Apr 18 00:13:49 2016]

Properties LastWrite : [Mon Apr 18 00:13:49 2016]

InstallDate : Fri Nov 20 01:56:01 2015 UTC

FirstInstallDate: Fri Nov 20 01:56:01 2015 UTC

DISK&VEN\_SONY&PROD\_DSC&REV\_1.00 (C68B200FB019&1)

LastWrite: Mon Apr 18 00:13:49 2016

DeviceDesc: DSC

Friendly: H:\

Mfg: Sony

Device Parameters LastWrite: [Mon Apr 18 00:13:49 2016]

LogConf LastWrite : [Mon Apr 18 00:13:49 2016]

Properties LastWrite : [Mon Apr 18 00:13:49 2016]

InstallDate : Fri Nov 20 01:56:03 2015 UTC

FirstInstallDate: Fri Nov 20 01:56:03 2015 UTC

DISK&VEN\_SONY&PROD\_DSC&REV\_1.00 (C68B200FB019&2)

LastWrite: Mon Apr 18 00:13:49 2016

DeviceDesc: DSC

Friendly: PMHOME

## SYSTEM OUTPUT

Mfg: Sony

Device Parameters LastWrite: [Mon Apr 18 00:13:49 2016]

LogConf LastWrite : [Mon Apr 18 00:13:49 2016]

Properties LastWrite : [Mon Apr 18 00:13:49 2016]

InstallDate : Fri Nov 20 01:55:58 2015 UTC

FirstInstallDate: Fri Nov 20 01:55:58 2015 UTC

ControlSet001\Control\DeviceClasses\{10497b1b-ba51-44e5-8318-a65c837b6661}

DISK&amp;VEN\_JMCR&amp;PROD\_SD&amp;REV\_5&amp;12E35340&amp;0&amp;000000

LastWrite: Wed Sep 23 03:08:50 2015

DISK&amp;VEN\_&amp;PROD\_&amp;REV\_2.20\0718011120035AF&amp;0

LastWrite: Mon Oct 19 13:06:21 2015

DISK&amp;VEN\_&amp;PROD\_&amp;REV\_PMAP\07032B5A180AA664&amp;0

LastWrite: Mon Sep 14 18:39:11 2015

DISK&amp;VEN\_&amp;PROD\_&amp;REV\_PMAP\070B43D2DE271C28&amp;0

LastWrite: Thu Oct 1 23:47:49 2015

DISK&amp;VEN\_&amp;PROD\_&amp;REV\_PMAP\070B43D9AB6E9253&amp;0

LastWrite: Sat Mar 19 22:25:27 2016

DISK&amp;VEN\_APPLE&amp;PROD\_IPOD&amp;REV\_2.70\000A27001CA9A995&amp;0

LastWrite: Thu Nov 19 17:48:07 2015

DISK&amp;VEN\_HP&amp;PROD\_USB\_FLASH\_DRIVE&amp;REV\_1.00\002354D46B97AC5102CF01C0&amp;0

LastWrite: Sat Sep 12 01:43:29 2015

DISK&amp;VEN\_PNY&amp;PROD\_USB\_2.0\_FD&amp;REV\_1100\ACB3HD1000000240&amp;0

LastWrite: Thu Oct 8 00:18:01 2015

DISK&amp;VEN\_PNY&amp;PROD\_USB\_2.0\_FD&amp;REV\_8192\AABA1ECC00001167&amp;0

LastWrite: Mon Oct 19 13:06:32 2015

DISK&amp;VEN\_SANDISK&amp;PROD\_CRUZER&amp;REV\_1.20\200544568018E7B0762E&amp;0

LastWrite: Mon Oct 26 09:56:12 2015

DISK&amp;VEN\_SANDISK&amp;PROD\_CRUZER&amp;REV\_8.02\17380302D5A10198&amp;0

LastWrite: Fri Feb 20 17:01:44 2015

DISK&amp;VEN\_SANDISK&amp;PROD\_CRUZER\_MICRO&amp;REV\_8.02\2243400CB8E0533D&amp;0

LastWrite: Wed Apr 6 14:25:07 2016

DISK&amp;VEN\_SONY&amp;PROD\_DSC&amp;REV\_1.00\C68B200FB019&amp;0

LastWrite: Fri Nov 20 01:55:59 2015

DISK&amp;VEN\_SONY&amp;PROD\_DSC&amp;REV\_1.00\C68B200FB019&amp;1

## SYSTEM OUTPUT

LastWrite: Fri Nov 20 01:56:02 2015

DISK&VEN\_SONY&PROD\_DSC&REV\_1.00\C68B200FB019&2

LastWrite: Fri Nov 20 01:55:58 2015

```

-----
ALERT: appinitdlls: Entry not blank: C:\WINDOWS\system32\nvinitx.dll
ALERT: appinitdlls: Entry not blank: C:\WINDOWS\SysWOW64\nvinit.dll
ALERT: cmd_shell: Clients\StartMenuInternet\IExplore.exe\shell\open\command warning:
C:\Program Files\Internet Explorer\iexplore.exe
WARNING: winlogon: Microsoft\Windows NT\CurrentVersion\Winlogon GinaDLL value found:
pssogina.dll
Alert: svc: AdobeFlashPlayerUpdateSvc has a WOW64 value: 1
Alert: svc: atashost has a WOW64 value: 1
Alert: svc: clr_optimization_v2.0.50727_32 has a WOW64 value: 1
Alert: svc: CVPNDRVA has a WOW64 value: 1
Alert: svc: gupdate has a WOW64 value: 1
Alert: svc: gupdatem has a WOW64 value: 1
Alert: svc: MozillaMaintenance has a WOW64 value: 1
Alert: svc: PerfHost has a WOW64 value: 1
Alert: svc: WIMMount has a WOW64 value: 1
ALERT: svcdll: wbem found in path: Winmgmt -> %SystemRoot%\system32\wbem\WMIsvc.dll
ALERT: svcdll: Relative path detected: WinHttpAutoProxySvc -> winhttp.dll
ALERT: cmd_shell: Clients\StartMenuInternet\IExplore.exe\shell\open\command warning:
C:\Program Files\Internet Explorer\iexplore.exe
Alert: svc: BrYNSvc has a WOW64 value: 1
Alert: svc: clr_optimization_v2.0.50727_32 has a WOW64 value: 1
Alert: svc: gupdate has a WOW64 value: 1
Alert: svc: gupdatem has a WOW64 value: 1
Alert: svc: MBAMProtector has a WOW64 value: 1
Alert: svc: MBAMScheduler has a WOW64 value: 1
Alert: svc: MBAMService has a WOW64 value: 1
Alert: svc: MBAMSwissArmy has a WOW64 value: 1
Alert: svc: MBAMWebAccessControl has a WOW64 value: 1
Alert: svc: McNaiAnn has a WOW64 value: 1
Alert: svc: McODS has a WOW64 value: 1
Alert: svc: mcpltsvc has a WOW64 value: 1
Alert: svc: McProxy has a WOW64 value: 1
Alert: svc: MozillaMaintenance has a WOW64 value: 1
Alert: svc: PDFProFiltSrvPP has a WOW64 value: 1
Alert: svc: PEFSservice has a WOW64 value: 1
Alert: svc: PerfHost has a WOW64 value: 1
Alert: svc: WIMMount has a WOW64 value: 1
ALERT: svcdll: wbem found in path: Winmgmt -> %SystemRoot%\system32\wbem\WMIsvc.dll
ALERT: svcdll: Relative path detected: WinHttpAutoProxySvc -> winhttp.dll

```